**VŠB – TECHNICKÁ UNIVERZITA OSTRAVA**
**Fakulta elektrotechniky a informatiky**
**Katedra telekomunikační techniky**

# Technologie AToM

# AToM Technology

**2011** **Zdeněk Pešek**

## Prohlášení

Prohlašuji, že tuto diplomovou práci jsem vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 5. 5. 2011

…….……

Zdeněk Pešek


## Poděkování:

Touto cestou bych chtěl vyjádřit poděkování mé rodině, která mě podporovala při studiích a vedoucímu diplomové práce Ing. Petru Machníkovi, Ph.D. za cenné rady a odborné vedení.

# Abstrakt a klíčová slova

## Abstrakt

Tato diplomová práce se zabývá popisem technologií AToM a VPLS. V první části je popsána technologie AToM a zařízení, které využívá pro tuto funkci. V dalším kroku je vysvětlena konfigurace MPLS jádra jako nosného protokolu pro obě technologie. Druhá část se zaměřuje na jednotlivé protokoly, které můžou být přenášeny přes MPLS jádro. Všechny protokoly jsou zde popsány, jsou zobrazeny jejich rámce, zapouzdření do MPLS a uvedeny realizace jednotlivých zapojení. Třetí část popisuje technologii VPLS, její význam a chování. Je zde uvedená základní konfigurace. Dále se práce v této části zaměřuje na návrh zapojení. Zkráceně je popsán hierarchický model, který umožňuje lépe škálovatelnost technologie.

## Klíčová slova

Virtuální privátní LAN služba, protokol pracující se značkami, přenos přes MPLS síť, směrovač, přepínač, virtuální okruh, připojený okruh, značka, relace, zdrojová IP adresa, cílová IP adresa, zapouzdření, tunel, rámec, paket, instance, soused

## Abstract

This diploma thesis focuses on the description of AtoM and VPLS technologies. The first part describes AtoM technology and device that are used for this function. The next step explains the configuration of MPLS core as the carrier protocol for the both technologies. The second part deals with the individual protocols that can be transported via MPLS core. This includes the description of all the protocols, their frames, encapsulation into MPLS and their suggestion of topology of network. The third part describes VPLS technology, its importance and behaviour. It also includes the initial configuration. The diploma thesis focuses here on the topology of network. Shortly it describes the hierarchical model that enables better scaling of the technology.

## Key words

Virtual private LAN services, Multiprotocol Label Switching, Any Transport over MPLS router, switch, virtual circuit, attachment circuit, label, session, source IP address, destination IP address, encapsulation, tunnel, frame, packet, instance, neighbor

# Seznam použitých symbolů a zkratek

| | | |
|---|---|---|
| **AC** | Attachment Circuit | Připojený okruh |
| **ARP** | Address Resolution Protocol | Protokol pro komunikaci na LAN |
| **ATM** | Asynchronous Transfer Mode | Typ protokolu druhé vrstvy ISO/OSI |
| **AToM** | Any Transport over MPLS | Technologie VPN na druhé vrstvě |
| **CDP** | Cisco Discovery Protocol | Protokol pro vyhledávání sousedů |
| **CE** | Customer Edge | Směrovač na straně zákazníka |
| **DLCI** | Data Link Connection Identifier | Identifikátor datové linky |
| **FR** | Frame Relay | Typ protokolu druhé vrstvy ISO/OSI |
| **HDLC** | High-Level Data Link Control | Typ protokolu druhé vrstvy ISO/OSI |
| **H-VPLS** | Hierarchical VPLS | Hierarchická VPLS |
| **IGP** | Interior Gateway Protocol | Interní směrovací protokol |
| **IP** | Internet Protocol | Internetový protokol |
| **IPv4** | Internet Protocol version 4 | Internetový protokol verze 4 |
| **IPv6** | Internet Protocol version 6 | Internetový protokol verze 6 |
| **LAN** | Local Area Network | Lokální síť |
| **LDP** | Label Distribution Protocol | Protokol pro distribuci značek |
| **LMI** | Local Management Interface | Rozhraní pro řízení |
| **LSP** | Label Switch Path | Cesta přepínaná podle značek |
| **LSR** | Label Switch Router | Směrovač používající LDP |
| **MAC** | Media Access Control | Identifikátor síťového rozhranní |
| **MPLS** | Multiprotocol Label Switching | Technologie pracující se značkami |
| **N-PE** | Network-Provider Edge | Typ směrovače u technologie HVPLS |
| **OSPF** | Open Short Path First | Typ interního směrovacího protokolu |
| **PE** | Provider Edge | Směrovač na straně poskytovatele |
| **PPP** | Point-to-Point Protocol | Typ protokolu druhé vrstvy ISO/OSI |
| **STP** | Spanning Tree Protokol | Protokol pro vyloučení smyček |
| **TLDP** | Targeted LDP | Cílená LDP relace |
| **TDP** | Tag Distribution Protocol | Starší protokol pro distribuci značek |
| **U-PE** | User-Provider Edge | Typ směrovače u technologie HVPLS |
| **VC** | Virtual Circuit | Virtuální okruh |
| **VFI** | Virtual Forwarding Instance | Instance virtuálního posílání |

| | | |
|---|---|---|
| **VLAN** | Virtual LAN | Virtuální lokální síť |
| **VPLS** | Virtual Private LAN Service | Virtuální privátní LAN služba |
| **VPN** | Virtual Private Network | Virtuální privátní síť |
| **VSI** | Virtual Switching Instance | Instance virtuálního přepínání |
| **VTP** | Virtual Trunking Protocol | Protokol pro práci s VLAN |

# Obsah


**1. Úvod ..... 1**

**2. Technologie Any Transport over MPLS ..... 2**

2.1 Seznámení s technologií AToM ..... 2

2.2 Konfigurace MPLS jádra ..... 3

**3. PPP over MPLS ..... 8**

3.1 Protokol PPP ..... 8

3.2 Metoda zapouzdření ..... 9

3.3 Konfigurace PPP over MPLS ..... 10

**4. HDLC over MPLS ..... 16**

4.1 Konfigurace HDLC over MPLS ..... 17

**5. Ethernet over MPLS ..... 19**

5.1 Formát Ethernetového rámce ..... 20

5.2 Konfigurace Ethernet over MPLS ..... 21

5.3 Ethernetové rámce při přenosu MPLS sítí ..... 25

**6. Frame Relay over MPLS ..... 28**

6.1 Metody Frame Relay over MPLS ..... 29

6.2 Konfigurace Frame Relay ..... 30

6.2 Zapouzdření Frame Relay rámce přes MPLS síť ..... 34

**7. Technologie VPLS ..... 38**

7.1 Základní princip VPLS ..... 39

7.1.1. Komponenty pro VPLS ..... 40

7.1.2 Zapouzdření Ethernetových rámců ..... 41

7.2 Základní konfigurace VPLS ..... 42

7.3 Tunelování protokolů druhé vrstvy ..... 44

7.4 Realizace VPLS ..... 45

7.5 Hierarchická VPLS ..... 52

7.5.1 H-VPLS s přístupovou vrstvou Dot1q tunel ..... 53

7.5.2 H-VPLS s přístupovou vrstvou MPLS ..... 56

**8. Srovnání technologií AToM a VPLS ..... 57**

**9. Závěr ..... 59**

**Literatura ..... 60**

**Seznam příloh ..... 61**

# 1. Úvod

Technologie Any Transport over MPLS (dále jen AToM) je řešení pro přenos rámců druhé vrstvy přes IP/MPLS páteřní sítě. MPLS je nosný protokol jak pro technologii AToM tak i pro VPLS, která je také popsána v této práci. MPLS služba předběhla ostatní WAN protokoly svou jednoduchostí a rychlostí. Její podstata je v tom, že vkládá mezi linkovou a síťovou vrstvu značku a podle této značky je řízen provoz v páteřní MPLS síti. Odpadá tedy nutnost rozbalování rámce až do síťové vrstvy, kde dochází k vyhledávání IP adres podle směrovací tabulky.

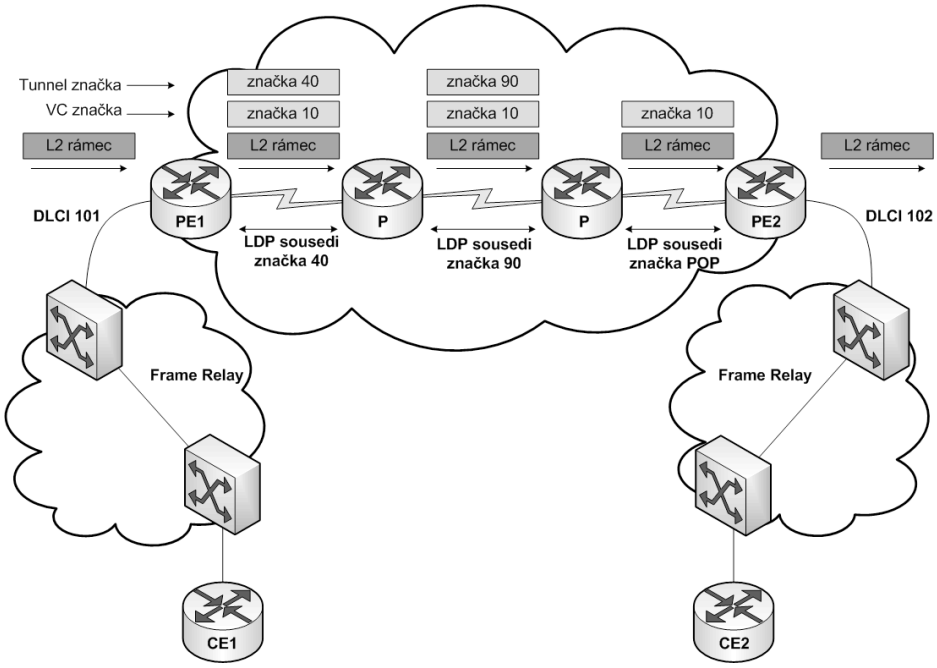
Jako první využila těchto výhod služba Traffic Engineering (TE). Ta dokázala směřovat IP provoz přes definovanou cestu MPLS sítí nabízející lepší vlastnosti a kontrolu než tradiční WAN technologie. Vlastnosti MPLS tak vydláždili příchod TE a podpory QoS do IP sítí. Další službou, která se prosadila do světa MPLS byla VPN služba. Začalo to s MPLS VPN definovanou v RFC 2547 a pokračovalo modely AToM a VPLS.

Služba AToM poskytuje další vlastnosti a těmi jsou oddělení provozu mezi zákazníky, dále je jednotlivý provoz zákazníka zapouzdřen do transportního tunelu typu bod-bod. Transportní tunely jsou vytvořeny pomocí signalizačních protokolů distribující značky. Tato služba dokáže přenášet provoz protokolů PPP, HDLC, Frame Relay, ATM a samozřejmě provoz Ethernetový. Další privátní služba VPLS, dokáže vícebodové spojení a pracuje pouze s Ethernetem, jelikož u sériových linek toto spojení není možné. Tato služba poskytuje všesměrovou doménu na zákazníka, jako by všechny sítě zákazníka byly připojeny do stejné LAN. Služba VPLS se rozšířila na hierarchický model neboli H-VPLS. Klasická VPLS vytváří virtuální okruhy mezi hraničními směrovači poskytovatele. Čím více roste síť poskytovatele, roste i počet hraničních směrovačů a s nimi taky počet virtuálních okruhů. Aby se tomuto zamezilo, byl vyvinut hierarchický model. Ten je rozdělen na síť VPLS a na síť přístupovou. K přístupové síti se připojují jednotliví zákazníci, nedochází tedy tak k velkému vytížení VPLS jádra.

# 2. Technologie Any Transport over MPLS

## 2.1 Seznámení s technologií AToM

Any Transport over MPLS (dále jen AToM) je technologie, kterou využívají poskytovatelé k přenosu provozu mezi dvěma zákazníky. Zařízení zákazníka je připojeno linkou typu bod-bod nebo Ethernetovou linkou ke směrovačům poskytovatele. Směrovače poskytovatele vytvářejí tunel mezi vzdálenými PE směrovači, provoz zákazníka je zapouzdřen na PE směrovačích do MPLS záhlaví. Dále je provoz přeposílán přes směrovače P, které se pouze starají o doručení k cílovému hraničnímu směrovači PE. Zde je zapouzdřený rámec rozbalen a poslán k zařízení zákazníka.




Obr. 2.1 Princip Any Transport over MPLS

Na obrázku 2.1 je zobrazena topologie MPLS jádra pro přenos Frame Relay. Jak můžeme vidět, rámec vstupující do PE směrovače je doplněn VC značkou, což je značka virtuálního okruhu. Tato značka zůstává stejná po celou dobu přenosu přes MPLS jádro a k ní se podle Label Switch Path (LSP) přidělují značky, které zajišťují cestu ke správnému směrovači PE. LSP je vlastně cesta daná těmito značkami. LSP má pouze jeden směr, pro opačný směr existuje jiná LSP. Mezi jednotlivými směrovači v MPLS jádru je definován protokol LDP a

protokol IGP což tvoří základ pro implementaci MPLS technologie. Na konci LSP, směrovač PE odstraní všechny značky a posílá pouze čistý rámec.

## 2.2 Konfigurace MPLS jádra

V této podkapitole je uvedena konfigurace MPLS páteře. Pokud jsou na všech směrovačích poskytovatele nastaveny základní konfigurace, jsou k rozhranním přiřazeny IP adresy, můžeme pokračovat vytvořením dynamického směrování mezi těmito směrovači. Jako směrovací protokol zde byl využit protokol Open Short Path First (OSPF), v tomto případě může být využitý jakýkoliv jiný interní směrovací protokol. Nakonec je popsána konfigurace protokolu LDP a MPLS funkce.

Pro funkci MPLS je důležitá konfigurace virtuálních rozhranní, tzv. Loobpack. Tyto rozhranní slouží jako identifikace směrovačů pro LDP protokol. Ujistěte se, že jsou Loopback rozhranní konfigurovány s maskou /32. Směrovače poskytovatele musí používat tuto masku na Loopback rozhranních, protože mezi těmito Loopback rozhranními jednotlivých směrovačů poskytovatele vzniká LDP relace a jsou touto maskou identifikovány.

Směrovací protokol OSPF spustíme příkazem *router ospf*, v dalším příkazu definujeme síťové adresy (přímo připojené sítě), které se budou distribuovat k sousedům a jejich wildcard což je převrácená hodnota masky, nakonec příkazu definujeme číslo OSPF oblasti, v těchto případech bude vždy nula, tedy páteřní oblast.

```
Router(config)# router ospf <číslo_procesu>
Router(config-router)# network <síťová_adresa> <wildcard> area
<oblast>
```

Příklad:

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 1.1.1.1 0.0.0.0 area 0
```

Po konfiguraci směrovacího protokolu na všech směrovačích v MPLS jádru je potřeba ověřit konektivitu mezi jednotlivými směrovači. Pro ověření můžeme využít výpis směrovací tabulky a příkaz ping. Konektivita musí být patrná i na všech virtuálních rozhranních Loopback.

```
Router# show ip route
Router# ping <IP adresa>
```

Funkci MPLS spustíme příkazem *mpls ip* v globálním konfiguračním režimu a také ji musíme spustit na jednotlivých rozhranních, na kterých bude docházet k přepínání rámců podle značek. Na novějších verzích IOS je tato funkce zapnuta defaultně.

```
Router(config)# mpls ip
Router(config-if)# mpls ip
```

Dále umožníme funkci protokolu LDP pro distribuci značek. Značky můžeme distribuovat pomocí protokolů LDP nebo TDP. Protokol TDP je předchůdce již zmíněného protokolu LDP.

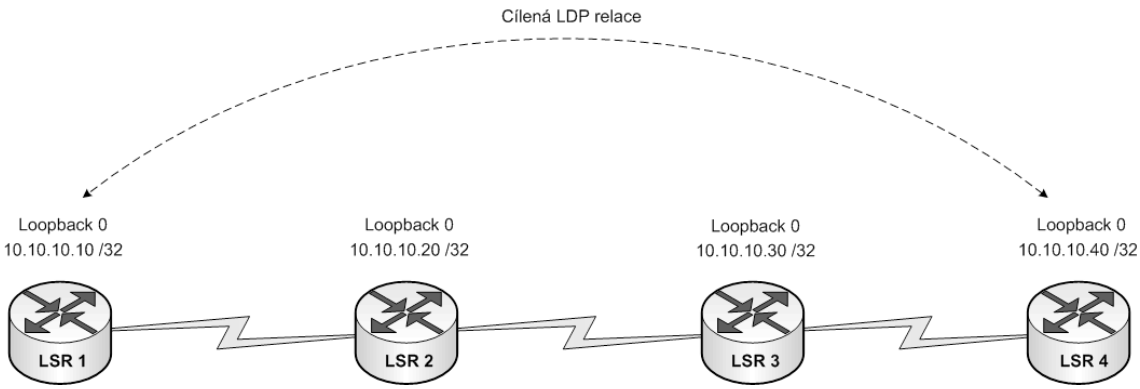
```
Router(config)# mpls label protocol ldp
```

Pro lepší orientaci je vhodné nastavit identifikaci směrovačů podle adresy Loopback.

```
Router(config)# mpls ldp router-id <loopback> force
```

Tímto je dokončena konfigurace MPLS jádra, mezi LDP sousedy dojde k distribuci značek. Většinou se LDP relace sestavuje mezi přímo připojené sousedy. TLDP (Targeted LDP) relace je rozdílná. Vyhledávání cílených LDP sousedů pomocí zpráv Hello je uskutečněno unicastovou adresou. Klasická LDP relace používá zprávy typu Hello s adresou pro multicast. Výsledně tedy můžeme sestavit LDP relaci mezi nepřímo připojené LSR routery. Směrovače tedy nemusí být na stejné podsíti. Je možné sestavit cílenou relaci taky mezi přímo připojené LSR routery. Cílená LDP relace se používá u technologie AToM a TE tunelů v MPLS VPN sítích. V případě použití technologie AToM, LDP relace musí existovat mezi každým párem PE (Provider Edge) routerů.

Cílená LDP relace mezi LDP sousedy může zlepšit konvergenci v porovnání s konvergencí s přímo připojenými LDP sousedy, pokud například kolísá linka. Při rozpadu linky mezi dvěma LSR směrovači dojde k ukončení LDP relace. Jestliže naopak použijeme cílenou LDP relaci pak je provoz směřován přes alternativní cestu a proto je LDP relace stále udržována. Cílená LDP relace je zobrazena na obr. 2.2.




Obr. 2.2 Cílená relace mezi nepřímo připojenými LSR směrovače

Vytvoření cílené LDP relace:

```
Router(config)# mpls ldp neighbor <IPadresa_vzdaleneho_PE>
targeted ldp
```

Kontrola nastavení pro MPLS:

```
Router# show mpls ldp neighbor
Router# show mpls forwarding-table
Router# show mpls ip binding
```

Kontrola nastavení pro protokol LDP:

```
Router# show mpls ldp bindings            /výpis
Router# show mpls ldp neighbor            /výpis LDP relací
```

Vysvětlení a popis jednotlivých příkazů pro kontrolu nastavení budou uvedeny v každém realizačním zapojení.

Abychom mohli nyní přenášet data 2. vrstvy od zákazníků přes MPLS jádro, musíme definovat zapouzdření mezi směrovači zákazníka a poskytovatele. Zapouzdření musí být na obou směrovačích shodné. Posledním úkonem je definování tunelu mezi jednotlivými PE směrovači příkazem *xconnect.*

```
Router(config-if)# encapsulation <typ>
```

Typy zapouzdření v těchto případech používáme PPP, defaultni HDLC, Frame Relay pro sériové linky a zapouzdření 802.1Q pro Ethernet.

Tunel na PE směrovačích můžeme vytvořit dvěma podobnými způsoby. První způsob zahrnuje vytvoření tunelu použitím tzv. pseudowire. Je to termín používaný pro transport jakýchkoliv rámců linkové vrstvy přes MPLS síť. Postup je následující, nejdříve vytvoříme pseudowire, kde definujeme jméno a zapouzdření, následně ji pomocí příkazu *xconnect* přiřadíme určitému rozhraní.

```
Router(config)# pseudowire-class <název>
Router(config-pw)# encapsulation mpls
Router(config-if)# xconnect <peer-router-id> <vcid> pw-class
                   <název>
```

Druhá možnost je definice tunelu přímo v příkazu *xconnec*t. Kde `Peer-router-id` je IP adresa konce tunelu, tedy PE směrovače kde bude okruh ukončen a `vc-id` je identifikátor virtuálního okruhu. Tento identifikátor musí být shodný na obou koncích okruhu, jinak by koncové PE směrovače nedokázaly tunel sestavit.

```
Router(config-if)# xconnect <peer-router-id> <vc-id>
                   encapsulation mpls
```

Poznámka:

Na vzniku pseudowire se původně podílel Luca Martini z firmy Cisco, původně obdržel požadavek pro přenos Frame Relay přes MPLS k zákazníkovi. Vytvořil tento prototyp, který byl později rozšířen na Asynchronous Transfer Mode (ATM), Ethernet VLAN, PPP a HDLC rámce. Proto jsou pseudowire známé také jako Martiniovi tunely.

Tímto je zcela dokončena konfigurace MPLS jádra. Nyní může páteř MPLS přenášet rámce linkové vrstvy pro definované zapouzdření.

Kontrola vytvořených tunelů na směrovačích PE:

```
Router# show mpls l2transport vc
```

Navržení topologie MPLS jádra závisí zcela na poskytovateli a samozřejmě na jeho finančních možnostech. V těchto řešeních jsou využity topologie hop-by-hop a hub and spoke. Směrovače zákazníků CE komunikují se směrovači PE poskytovatele a směrovače P se pouze podílí na přepínání rámců k cílovému PE směrovači. Pokud poskytujeme přenos pro více zákazníků s rozdílnými technologiemi, je lepší posílit jádro MPLS více P směrovači propojeným mezi sebou, tím se rozloží provoz mezi tyto směrovače a dokonce můžeme definovat cestu pro jednotlivé zákazníky.

# 3. PPP over MPLS

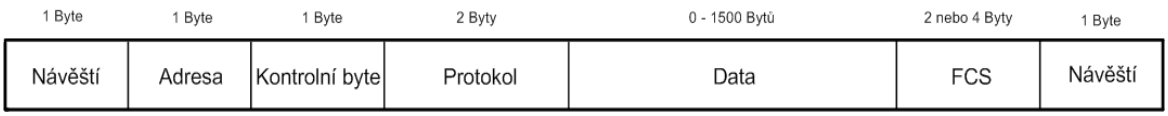
## 3.1 Protokol PPP

V této kapitole je popsán protokol PPP, jeho rámec, je zde uvedena jednoduchá topologie a implementace pro přenos PPP rámců přes MPLS jádro.

Point-to-Point Protocol zkráceně PPP je protokol druhé vrstvy ISO/OSI modelu. Obvykle je používán mezi dvěma síťovými uzly. Hojně je také využíván pro spojení LAN-to-WAN sítí. Protokol poskytuje autentizaci, šifrování a kompresi. PPP může využívat spoustu typů fyzických propojení jako sériový kabel, telefonní linky, trunk linky, specializované rádiové linky a dokonce i optické linky jako SONET. Mnoho internetových poskytovatelů používají PPP pro přístup zákazníků využívající vytáčený (dial-up) přístup k internetu. Protokol je obvykle používán jako protokol linkové vrstvy přes synchronní i asynchronní okruhy, kde nahrazuje starší technologie. Protokol PPP byl navržen pro práci s více protokoly síťové vrstvy, tudíž může být využíván jak pro IP (IPv4, IPv6) sítě, tak pro další nepříliš známé jako jsou Internetwork Packet Exchange (IPX) a AppleTalk.

Zapouzdření PPP je složeno ze tří komponent [1]:

- PPP používá HDLC protokol jako základní zapouzdření datagramů
- Link Control protocol (LCP) se stará o navázání, konfiguraci a testování linkového spojení
- Network Control Protocol (NCP) zapouzdřuje protokoly síťové vrstvy (IP, IPX, AppleTalk).




Obr. 3.1 Rámec protokolu PPP

Návěští: indikuje začátek nebo konec rámce, pole obsahuje binární sekvenci 01111110

Adresa: sériové linky typu PPP a HDLC posílají rámec všesměrovým vysíláním, tudíž pole obsahuje binární formu 11111111

Protokol: dva bajty identifikující zapouzdřený protokol

Data: paket specifikovaný v poli Protokol

FCS: Frame Check Sequence, výchozí nastavení 2 byty, 4 byty mají lepší detekci chyb

## 3.2 Metoda zapouzdření

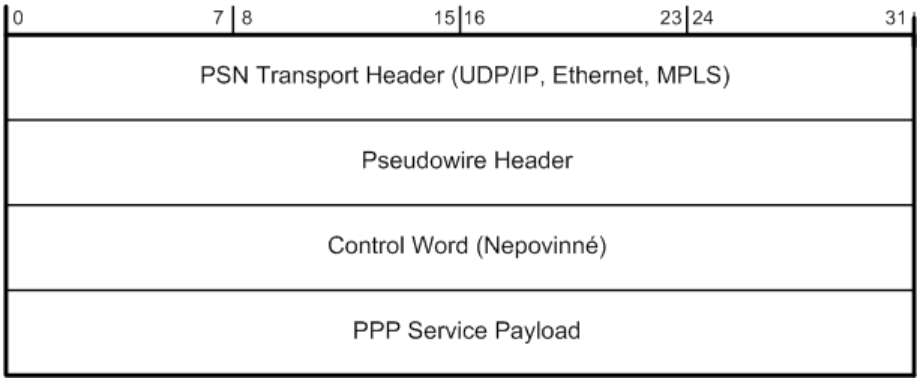
Tato podkapitola popisuje všeobecný formát pro zapouzdření PPP přes MPLS pseudowire [2]. Zapouzdření je shodné i pro ostatní protokoly.

**PSN Transport Header** liší se v závislosti na konkrétní technologii tunelování, slouží k přepravě zapouzdřené PPP informace přes paketové sítě.

**Pseudowire Header** značka pro virtuální okruh, v případě MPLS se jedná o MPLS značku přidávanou k rámci jako první (bottom label).

**Control Word** použitý pro kontrolní informace protokolu a sekvenčního čísla, povinná pouze pro Frame Relay a ATM AAL5

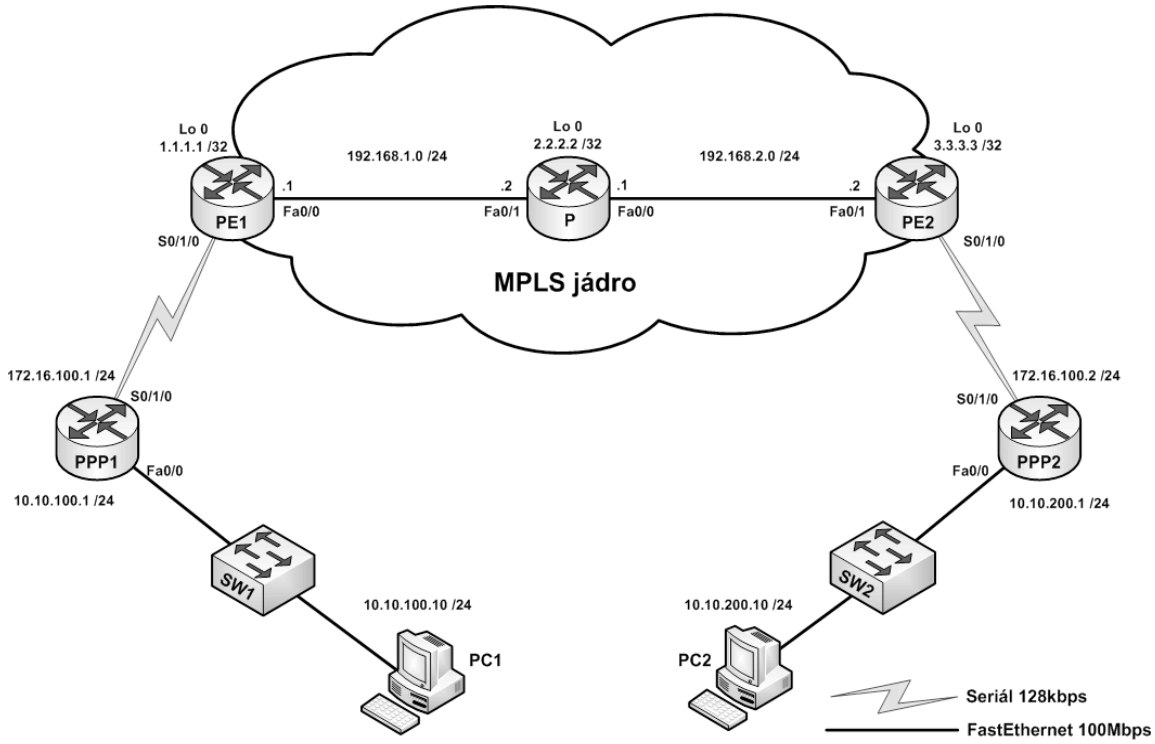
**PPP Service Payload** data linkové vrstvy, obsahuje rámec z obr. 3.1




Obr. 3.2 Obecné zapouzdření rámce PPP

## 3.3 Konfigurace PPP over MPLS

Tato kapitola obsahuje jednoduchou topologii páteřní sítě MPLS pro přenos rámců protokolu PPP. Jádro MPLS je složeno ze tří směrovačů. Dva jsou hraniční PE1, PE2 a mezi nimi je směrovač P. K hraničním směrovačům jsou připojeny přes sériovou linku zákaznické směrovače PPP1 a PPP2. Z těchto zákaznických směrovačů jsou přes přepínače SW1 a SW2 připojeny koncové stanice PC1 a PC2.




Obr. 3.3 Topologie pro přenos PPP přes MPLS

Obecná konfigurace MPLS jádra je popsána v kapitole 2.2. Zde si popíšeme nezbytné kroky pro konfiguraci této topologie pro přenos PPP přes MPLS jádro. Celé konfigurace všech zařízení jsou obsaženy v přílohách. Nejdříve nastavíme všem rozhraním příslušné IP adresy včetně Loopbacků.

Příklad konfigurace rozhranní pro směrovač PE1:

```
PE1 (config)# interface Fa0/0
PE1 (config-if)# ip address 192.168.1.1 255.255.255.0
PE1 (config-if)# no shutdown

PE1 (config)# interface Loopback 0
PE1 (config-if)# ip address 1.1.1.1 255.255.255.255
```

Při konfiguraci rozhranní Loopback není potřeba zadávat příkaz *no shutdown.* Rozhranní je pouze softwarové a proto je aktivní hned při jeho konfiguraci.
Nyní, když máme ke všem rozhranním přiřazenou IP adresu je na řadě konfigurace směrovacího protokolu OSPF. Konfigurace spočívá v definování všech přímo připojených sítí.

Příklad konfigurace směrovacího protokolu OSPF pro směrovač PE1:

```
PE1 (config)# router ospf 1
PE1 (config-router)# network 192.168.1.0 0.0.0.255 area 0
PE1 (config-router)# network 1.1.1.1 0.0.0.0 area 0
```

Po konfiguraci na všech směrovačích v MPLS jádru začnou směrovače rozesílat svoje směrovací tabulky a tím dojde k sestavení sousedství mezi všemi směrovači definované v autonomním systému 1. Správnou funkci ověříme vypsáním směrovací tabulky.

Ve výpisu na další straně, můžeme vidět všechny dosažitelné sítě ze směrovače PE1. Adresy s maskou /32 jsou adresy Loopback rozhranní jednotlivých směrovačů poskytovatele. Konektivitu můžeme taky otestovat příkazem ping.

Ověření funkce směrovacího protokolu OSPF:

```
Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 192.168.1.2, 00:00:10, FastEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/3] via 192.168.1.2, 00:00:10, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/2] via 192.168.1.2, 00:00:10, FastEthernet0/0
PE1(config-router)#
PE1#ping
*Oct  7 06:33:15.919: %SYS-5-CONFIG_I: Configured from console by console
PE1#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
PE1#
```

Dále pokračujeme s konfigurací protokolu LDP a funkcí MPLS. Jak už bylo zmíněno v kapitole 2.2, funkci MPLS musíme zapnout jak v globálním konfiguračním módu tak na jednotlivých rozhranních podílejících se na funkci MPLS.

Příklad zpřístupnění funkce MPLS na směrovači PE1:

```
PE1 (config)# mpls ip
PE1 (config)# interface Fa0/0
PE1 (config-if)# mpls ip
```

Příklad konfigurace LDP protokolu na směrovači PE1:

```
PE1 (config)# mpls label protocol ldp
PE1 (config)# mpls ldp router-id loopback 0 force
PE1 (config)# mpls ldp neighbor 3.3.3.3 targeted ldp
```

Správnou funkci protokolu LDP a MPLS můžeme ověřit v jednotlivých výpisech:

```
PE1#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     2.2.2.2/32       0             Fa0/0      192.168.1.2
17     17            3.3.3.3/32       0             Fa0/0      192.168.1.2
18     Pop Label     192.168.2.0/24   0             Fa0/0      192.168.1.2
19     No Label      l2ckt(100)       27832         Se0/1/0    point2point
PE1#
```

Z příkazu můžeme vyčíst, že pro každý prefix je určena značka. Pop label je funkce, která odstraňuje poslední přidanou značku z paketu. Jsou zde určeny také výstupní rozhranní, v případě směrovače PE1 se jedná vždy o rozhranní Fa0/0 a další směrovač (Next Hop) je směrovač s IP adresou 192.168.1.2 tudíž se jedná o směrovač P.

Ověření LDP sousedů:

```
PE1#sh mpls ldp neighbor
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 2.2.2.2.62521 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 34/34; Downstream
        Up time: 00:23:10
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.1.2
        Addresses bound to peer LDP Ident:
          192.168.2.1     192.168.1.2     2.2.2.2
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 3.3.3.3.45576 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 26/25; Downstream
        Up time: 00:14:34
        LDP discovery sources:
          Targeted Hello 1.1.1.1 -> 3.3.3.3, active, passive
        Addresses bound to peer LDP Ident:
          192.168.2.2     3.3.3.3
```

V tomto výpisu můžeme pozorovat LDP sousedství mezi jednotlivými směrovači. V první části výpisu je zobrazeno klasické LDP sousedství navázané mezi směrovači PE1 a P. Protokol LDP používá komunikační port 646. Ve druhé části je výpis cílené LDP relace mezi směrovači PE1 a PE2.

Funkce MPLS v jádře poskytovatele je tedy zcela funkční, nyní se zaměříme na konfiguraci zákaznických směrovačů. Podle známého scénáře nastavíme IP adresu na sériovém rozhranní. Na straně DCE nezapomeňme nastavit hodinový signál pomocí příkazu *clock rate*. Poté vytvoříme L2 tunel mezi směrovači PE1 a PE2.

Konfigurace zákaznického směrovače PPP1:

```
PPP1 (config)# interface serial 0/1/0
PPP1 (config-if)# ip address 172.16.100.1 255.255.255.0
PPP1 (config-if)# encapsulation ppp
PPP1 (config-if)# clock rate 128000
PPP1 (config-if)# no shutdown
```

Konfigurace L2 tunelu na směrovači PE1:

```
PE1 (config)# interface serial 0/1/0
PE1 (config-if)# encapsulation ppp
PE1 (config-if)# xconnect 3.3.3.3 200 encapsulation mpls
PE1 (config-if)# no shutdown
```

Na sériových rozhranních směrovačů PE1 a PE2 není potřeba nastavovat IP adresu, jedná se o tunel druhé vrstvy ISO/OSI modelu.

Konfigurace L2 tunelu na směrovači PE2:

```
PE2 (config)# interface serial 0/1/0
PE2 (config-if)# encapsulation ppp
PE2 (config-if)# xconnect 1.1.1.1 200 encapsulation mpls
PE2 (config-if)# no shutdown
```

Ověření L2 tunelu mezi směrovači PE1 a PE2:

```
PE1#sh mpls l2transport vc 200

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Se0/1/0        PPP                        3.3.3.3         200        UP
```

Výpis nám zobrazuje způsob zapouzdření, cílovou IP adresu okruhu (Dest address), identifikátor virtuálního okruhu (VC ID) a status okruhu, který je aktivní (UP).

Poslední úkonem je nastavení směrování mezi zákaznickými směrovači PPP1 a PPP2. Přiřadíme IP adresy pracovním stanicím, přiřadíme jim defaultní bránu.

Nastavení základních parametrů na pracovní stanici PC1 a ověření funkčnosti celé topologie:

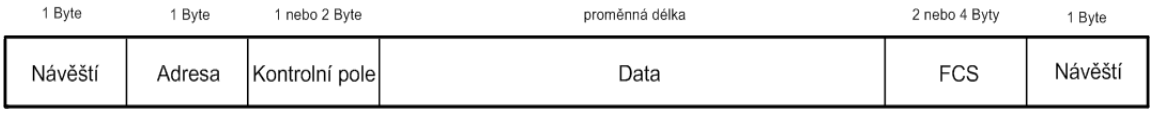
```
root@student-desktop:~# ifconfig eth0 10.10.100.10 netmask 255.255.255.0 up
root@student-desktop:~# route add default gw 10.10.100.1
root@student-desktop:~# ping 10.10.200.10
PING 10.10.200.10 (10.10.200.10) 56(84) bytes of data.
64 bytes from 10.10.200.10: icmp_seq=1 ttl=62 time=31.1 ms
64 bytes from 10.10.200.10: icmp_seq=2 ttl=62 time=24.4 ms
64 bytes from 10.10.200.10: icmp_seq=3 ttl=62 time=24.5 ms
64 bytes from 10.10.200.10: icmp_seq=4 ttl=62 time=24.4 ms
64 bytes from 10.10.200.10: icmp_seq=5 ttl=62 time=24.5 ms
```

# 4. HDLC over MPLS

Protokol HDLC je jeden z nejpoužívanějších protokolů linkové vrstvy. Protokol je založen na protokolu SDLC (Synchronous Data Link Control) firmy IBM. Je to bitově orientovaný protokol, provádí detekci chyb i řízení toku dat. HDLC protokol poskytuje spojově i nespojově orientované služby. Cisco směrovače používají HDLC protokol jako výchozí zapouzdření pro sériová rozhranní.

**Zapouzdření HDLC rámce:**

| | |
|---|---|
| Návěští: | bitová posloupnost 01111110, ohraničuje rámec |
| Adresa: | označuje cílovou stanici, v sítích typu bod-bod je adresa všesměrová 11111111 |
| Kontrolní pole: | značí typ HDLC rámce |
| Data: | nesou informace o paketu |
| FCS: | kontrolní součet pro ověření správného přenosu |




Obr. 4.0 Zapouzdření HDLC rámce

Konfigurace HDLC protokolu přes MPLS jádro je shodná s konfigurací protokolu PPP. Celá konfigurace je uvedena v předchozí kapitole. V této kapitole je uvedena stejná topologie jádra MPLS, takže se zaměříme pouze na konfiguraci zákaznických směrovačů a koncových směrovačů poskytovatele.

## 4.1 Konfigurace HDLC over MPLS

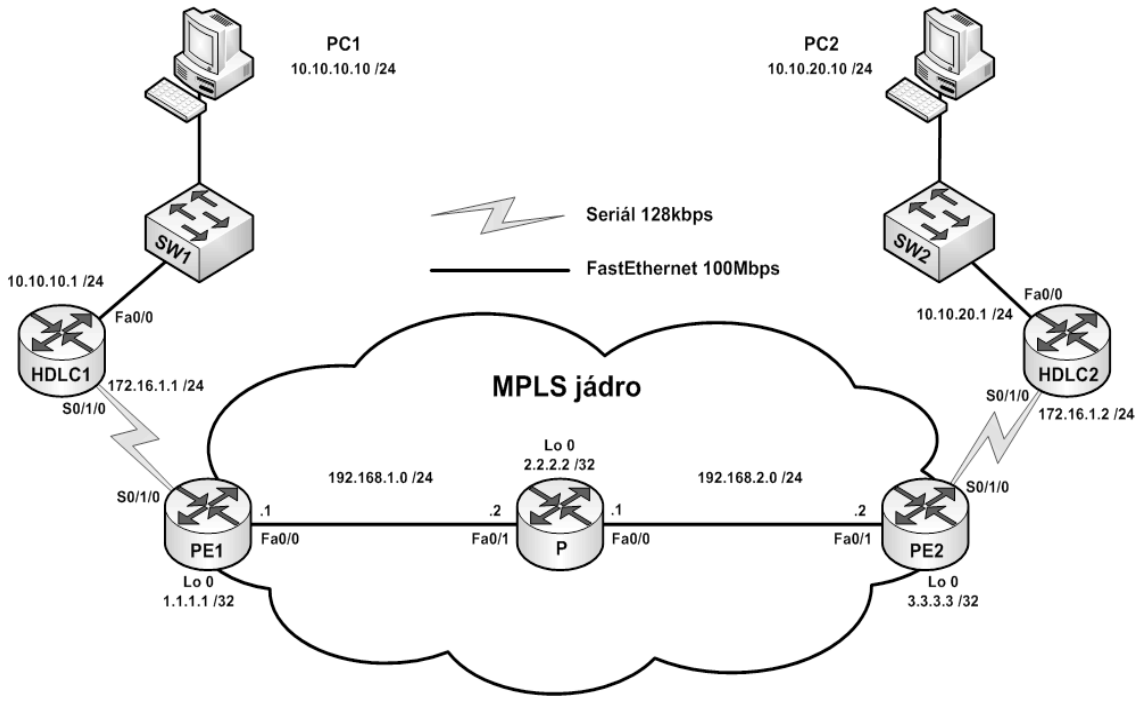
Na obr. 4.1 je zobrazena topologie jádra MPLS a dvou zákaznických sítí HDLC1 a HDLC2. Konfigurace spočívá ve správném nastavení zapouzdření. Jak jsem již zmínil dříve, směrovače Cisco využívají jako výchozí zapouzdření právě protokol HDLC. Zapouzdření používané sériovým rozhranním pro jistotu můžeme zkontrolovat příkazem:

```
HDLC1# show interface serial <číslo>
```

Ve výpisu příkazu najdeme poznámku Encapsulation HDLC. Pokud bude rozhranní používat jiný typ zapouzdření, upravíme to následujícím příkazem:

```
HDLC1(config)# interface serial 0/1/0
HDLC1(config-if)# encapsulation hdlc
```

Zapouzdření musí být shodné na obou koncích sériové linky tedy jak na směrovači HDLC tak na směrovači PE.




Obr. 4.1 Topologie pro přenos HDLC rámců přes MPLS jádro

Konfigurace L2 tunelu na směrovači PE1:

```
PE1 (config)# interface serial 0/1/0
PE1 (config-if)# encapsulation hdlc
PE1 (config-if)# xconnect 3.3.3.3 100 encapsulation mpls
PE1 (config-if)# no shutdown
```

Stejným způsobem konfigurujeme směrovače HDLC2 a PE2. Konec tunelu v případě směrovače PE2 je adresa 1.1.1.1 v příkazu *xconnect.* Nyní ověříme nastavení tunelu.

Ověření L2 tunelu mezi směrovači PE1 a PE2:

```
PE1#sh mpls l2transport vc 100

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Se0/1/0        HDLC                       3.3.3.3         100        UP
```

Tunel mezi koncovými směrovači PE je aktivní. Přes MPLS jádro přenášíme lokální okruh s HDLC zapouzdřením.

```
root@student-desktop:~# ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
root@student-desktop:~# route add default gw 10.10.10.1
root@student-desktop:~# ping 10.10.20.10
PING 10.10.20.10 (10.10.20.10) 56(84) bytes of data.
64 bytes from 10.10.20.10: icmp_seq=1 ttl=254 time=29.1 ms
64 bytes from 10.10.20.10: icmp_seq=2 ttl=254 time=24.8 ms
64 bytes from 10.10.20.10: icmp_seq=3 ttl=254 time=24.8 ms
64 bytes from 10.10.20.10: icmp_seq=4 ttl=254 time=24.8 ms
64 bytes from 10.10.20.10: icmp_seq=5 ttl=254 time=24.8 ms
```

# 5. Ethernet over MPLS

Nejpoužívanější technologií v LAN sítích je bezesporu Ethernet. Pro svou jednoduchost, pořizovací cenu vytlačil z této pozice ostatní méně známé technologie jako Token Ring a další.

Ethernetové propojení zákaznických sítí přes MPLS jádro je pouze typu bod-bod. Pro každé takové spojení musíme definovat L2 tunel vstupního a výstupního směrovače poskytovatele. Toto řešení můžeme přirovnat k přemostění LAN-to-LAN přes bod-bod WAN linku. Spojení není vícebodové, a proto zde nemůžeme využívat všesměrové vysílání.

Ethernetové sítě připojené ke směrovačům poskytovatele můžou být dvojího typu. Ethernet mód a IEEE 802.1Q VLAN mód. Protokol LDP signalizuje pro každý mód rozdílný typ virtuálního okruhu (VC) a typ pseudowire (PW). O tuto signalizaci se stará cílená LDP relace hraničních PE směrovačů. Ty se domluví na typu přenášeného linkového okruhu a podle toho okruh definují [3]. Typ virtuálního okruhu (VC Type) pro Ethernet mód je 5 a pro VLAN mód je to 4.

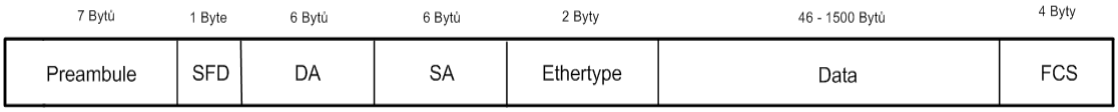
Pokud směrovače PE pracují v Ethernet módu, tunel mezi hraničními PE směrovači je vytvořen na jednotlivých fyzických rozhranních směrem k zákazníkovi. Takto vytvořený tunel může přenášet neoznačený Ethernetový provoz nebo označený provoz pro více VLAN mezi dvěma zákaznickými sítěmi, tunel tedy může pracovat jako trunk. Pokud chceme využit pseudowire jako trunk musíme na zákaznických směrovačích vytvořit jednotlivá pod-rozhranní a použít 802.1Q zapouzdření pro každou VLAN. V Ethernet módu může ale nemusí být VLAN hlavička součástí rámce. I když je rámec označen hlavičkou k určité virtuální síti, PE směrovače ji nezkoumají a posílají data transparentně na konec tunelu.

Ethernet VLAN mód je tvořen na PE směrovačích konfigurací pod-rozhranní a jejich zapouzdřením 802.1Q. Pro každé pod-rozhranní můžeme definovat tunel do jiné destinace. Každá virtuální síť má svoji pseudowire a může být směrována odlišně. Toto řešení je provedeno prakticky v této kapitole. U tohoto módu můžeme využívat zajímavou vlastnost, tzv. VLAN ID Rewrite [3]. Tato funkce je dobře využitelná, pokud máme na obou koncích tunelu definovanou rozdílnou identifikaci VLAN ID. V tomto případě dojde k jejich přepsání.

## 5.1 Formát Ethernetového rámce

**Zapouzdření Ethernetového rámce:**

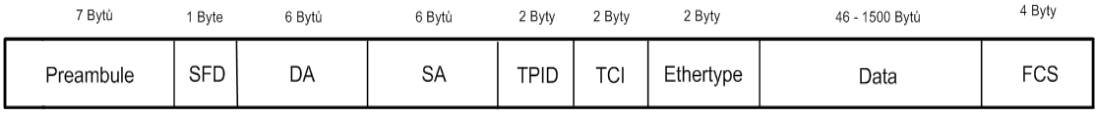
| | |
|---|---|
| Preambule: | 7 oktetů obsahující binární změnu 10101010 |
| SFD (Start of Frame Delimeter): | označení začátku rámce, oktet 10101011 |
| DA (Destination Address): | MAC adresa cílového síťového rozhranní |
| SA (Source Address): | MAC adresa zdrojového síťového rozhranní |
| Ethertype: | typ protokolu použitý ve vyšší vrstvě |
| Data: | min. délka 46 oktetů a max. 1500 oktetů |
| FCS (Frame Check Sequence): | 32bitový kontrolní kód, ověřuje správnost přijatých dat |




Obr. 5.1a Zapouzdření Ethernetového rámce

**Zapouzdření IEEE 802.1Q VLAN:**

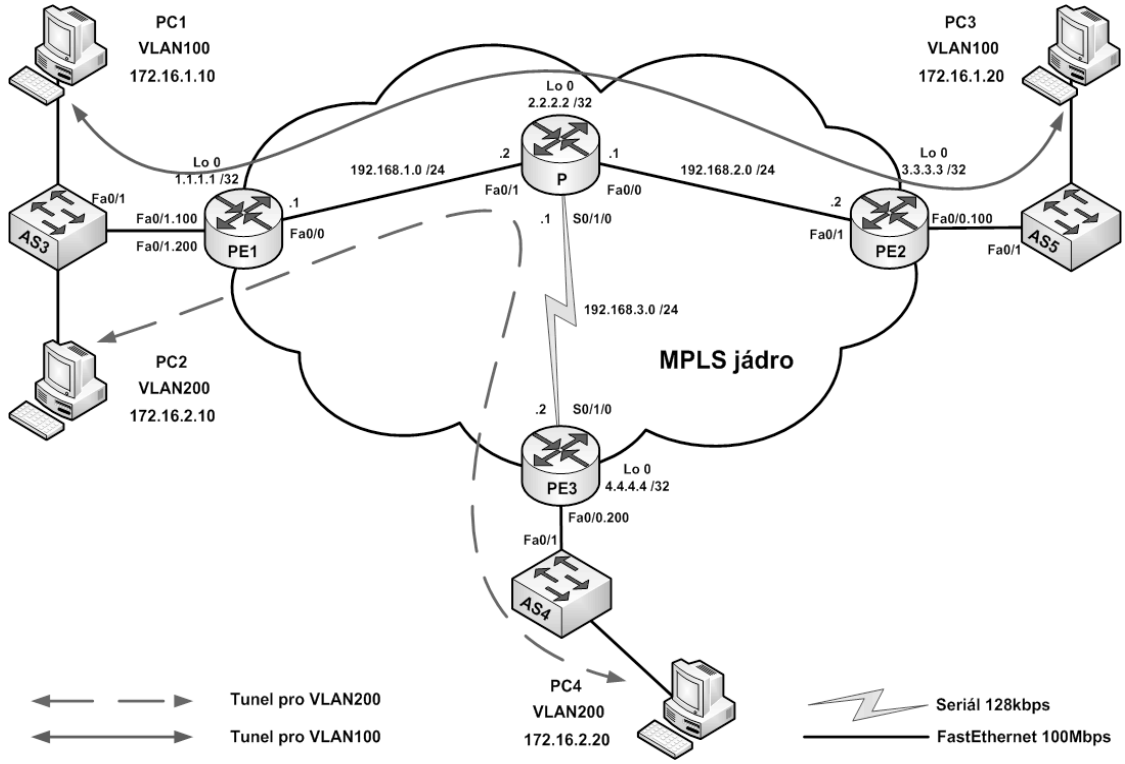
Rámec je rozšířen o dvě pole, které nám definují 802.1Q VLAN hlavičku. Tyto 4 byty se také nazývají VLAN tag.




Obr. 5.1b Zapouzdření EEE 802.1Q rámce

## 5.2 Konfigurace Ethernet over MPLS

V této podkapitole je popsána konfigurace pro přenos dvou virtuálních sítí VLAN100 a VLAN200 přes MPLS jádro. Topologie MPLS jádra je uspořádána jako hub and spoke. K jednomu P směrovači jsou připojeny tři směrovače PE. Tunel pro VLAN100 je vytvořen na pod-rozhranních směrovačů PE1 a PE2 a tunel VLAN200 je vytvořen mezi směrovači PE1 a PE3.




Obr. 5.2 Topologie pro Ethernet over MPLS ve VLAN módu

Konfigurace MPLS jádra je stejná jako v případě PPP. Cílená LDP relace je vytvořena mezi směrovači PE1 – PE2 pro VLAN100 a PE1 – PE3 pro VLAN200.

Cílená LDP relace mezi PE1 – PE2:

```
PE1 (config)# mpls ldp neighbor 3.3.3.3 targetted ldp
PE2 (config)# mpls ldp neighbor 1.1.1.1 targetted ldp
```

Cílená LDP relace mezi PE1 – PE3:

```
PE1 (config)# mpls ldp neighbor 4.4.4.4 targetted ldp
PE3 (config)# mpls ldp neighbor 1.1.1.1 targetted ldp
```

Ověření LDP sousedů a navázání cílene LDP relace:

```
PE1#sh mpls ldp neighbor
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 2.2.2.2.62521 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 184/185; Downstream
        Up time: 02:33:17
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.1.2
        Addresses bound to peer LDP Ident:
          192.168.2.1     192.168.1.2     2.2.2.2         192.168.3.1
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 3.3.3.3.45576 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 183/181; Downstream
        Up time: 02:24:42
        LDP discovery sources:
          Targeted Hello 1.1.1.1 -> 3.3.3.3, active, passive
        Addresses bound to peer LDP Ident:
          192.168.2.2     3.3.3.3
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 4.4.4.4.58119 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 62/63; Downstream
        Up time: 00:45:44
        LDP discovery sources:
          Targeted Hello 1.1.1.1 -> 4.4.4.4, active, passive
        Addresses bound to peer LDP Ident:
          192.168.3.2     4.4.4.4
```

Z výpisu je patrné, že směrovač PE1 navázal tři LDP spojení. První část popisuje lokální LDP relaci mezi směrovači PE1 a P. Druhá a třetí část zobrazuje cílenou LDP relaci mezi směrovači PE1 – PE2 a PE1 – PE3.

Tunely mezi jednotlivými směrovači vytvoříme na jejich pod-rozhranních. Na směrovači PE1 jsou vytvořeny dvě pod-rozhranní. Pod-rozhranní fa0/1.100 vytváří tunel pro VLAN100 a fa0/1.200 je tunel pro VLAN200. Pro přehlednost jsou pod-rozhranní označeny jako virtuální sítě.

Konfigurace L2 tunelu na směrovači PE1 pro VLAN100:

```
PE1 (config)# interface fa0/1.100
PE1 (config-subif)# encapsulation dot1q 100
PE1 (config-subif)# xconnect 3.3.3.3 100 encapsulation mpls
PE1 (config-subif)# exit
```

Konfigurace L2 tunelu na směrovači PE1 pro VLAN200:

```
PE1 (config)# interface fa0/1.200
PE1 (config-subif)# encapsulation dot1q 200
PE1 (config-subif)# xconnect 4.4.4.4 200 encapsulation mpls
PE1 (config-subif)# exit
```

Pod-rozhranní zapneme příkazem *no shutdown* na rozhranní fa 0/1

```
PE1 (config)# interface fa0/1
PE1 (config-if)# no shutdown
```

Obdobně konfigurujeme druhé konce tunelů na směrovačích PE2 a PE3 s jednou malou změnou. V příkazu *xconnect* pro oba směrovače PE2 a PE3 definujeme konec tunelů (peer-router-id) adresou Loopback 0 směrovače PE1 což je adresa 1.1.1.1.

Ověření L2 tunelů na směrovači PE1:

```
PE1#sh mpls l2transport vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Fa0/1.100      Eth VLAN 100               3.3.3.3         100        UP
Fa0/1.200      Eth VLAN 200               4.4.4.4         200        UP
PE1#
```

Z výpisu nyní můžeme usuzovat vytvoření dvou tunelů na směrovači PE1, oba jsou aktivní. Cílová IP adresa pro tunel s identifikátorem 100 je Loopback adresa směrovače PE2 a tunel s identifikátorem 200 patří cílovému směrovači PE3 respektive na jeho Loopback adresu.

MPLS jádro je zcela funkční, tunely pro jednotlivé VLAN jsou aktivní. Přistoupíme tedy ke konfiguraci přepínačů AS3, AS4 a AS5. Konfigurace spočívá v nastavení rozhranní fa0/1 na všech těchto přepínačích jako trunk. Přepínač AS3 přenáší ke směrovači PE1 obě VLAN 100 a 200.

Vytvoření virtuálních sítí na přepínači AS3:

```
AS3 (config)# vlan 100
AS3 (config)# vlan 200
```

Konfigurace rozhranní přepínače AS3 jako trunk:

```
AS3 (config)# interface fa0/1
AS3 (config-if)# switchport mode trunk
AS3 (config-if)# switchport trunk allowed vlan 100,200
AS3 (config-if)# no shutdown
```

Nyní rozhranní fa0/1 přepínače AS3 umožňuje přenos VLAN100 a VLAN200 ke směrovači PE1. Rozhranní fa0/1 na přepínači AS5 konfigurujeme pouze pro přenos VLAN100 a přepínač AS4 pro přenos VLAN200. Posledním úkonem je přiřazení pracovních stanic do správných VLAN.

Konfigurace přístupových rozhranní pro pracovní stanice:

PC1:
```
AS3 (config)# interface fa0/2
AS3 (config-if)# switchport mode access
AS3 (config-if)# switchport access vlan 100
```

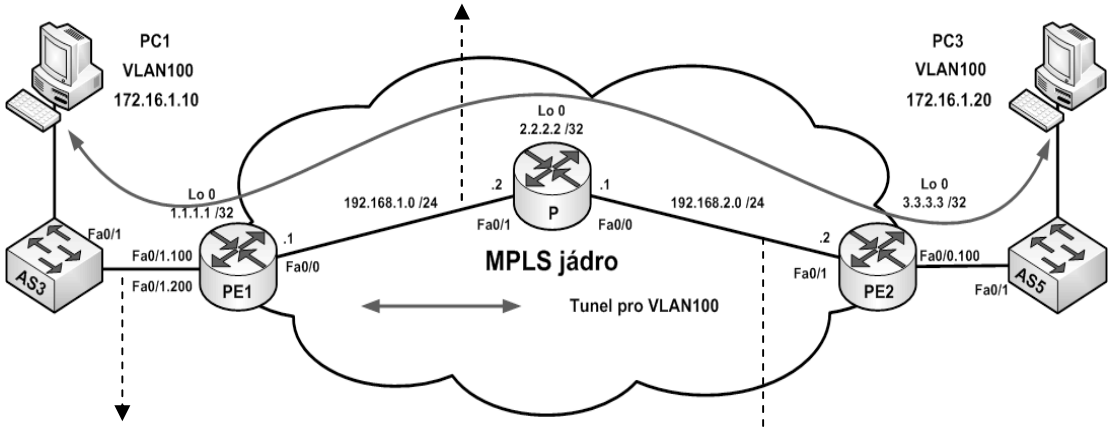
PC2:
```
AS3 (config)# interface fa0/3
AS3 (config-if)# switchport mode access
AS3 (config-if)# switchport access vlan 200
```

Stejným způsobem nastavíme přepínače AS4 a AS5.

## 5.3 Ethernetové rámce při přenosu MPLS sítí

Tato kapitola popisuje zapouzdření rámce při přenosu mezi zákaznickými sítěmi pro VLAN100. Provoz byl zachycen paketovým analyzátorem Wireshark a byl prováděn na třech místech topologie. Nejdříve je zachycen "čistý" Ethernetový rámec před příchodem do směrovače PE1. Dále je rozebrán rámec mezi směrovači PE1 a P, kde je k rámci přiřazeno MPLS záhlaví. Třetí část rozboru je zachycen mezi směrovači P a PE2, kde směrovač PE2 využívá funkce PHP a posílá zprávu směrovači P, ať odstraní poslední přidanou značku.

```
Frame 22 (128 bytes on wire, 128 bytes captured)
Ethernet II, Src: Cisco_4b:57:dc (00:17:5a:4b:57:dc), Dst: Cisco_4b:52:f3 (00:17:5a:4b:52:f3)
  Destination: Cisco_4b:52:f3 (00:17:5a:4b:52:f3)
  Source: Cisco_4b:57:dc (00:17:5a:4b:57:dc)
  Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 0, TTL: 255
MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 1, TTL: 255
PW Ethernet Control Word
Ethernet II, Src: FujitsuS_af:78:7b (00:30:05:af:78:7b), Dst: FujitsuS_8e:5e:4f (00:30:05:8e:5e:4f)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 100
Internet Protocol, Src: 172.16.1.10 (172.16.1.10), Dst: 172.16.1.20 (172.16.1.20)
Internet Control Message Protocol
```




```
Frame 36 (102 bytes on wire, 102 bytes captured)
Ethernet II, Src: FujitsuS_af:78:7b (00:30:05:af:78:7b), Dst: FujitsuS_8e:5e:4f (00:30:05:8e:5e:4f)
  Destination: FujitsuS_8e:5e:4f (00:30:05:8e:5e:4f)
  Source: FujitsuS_af:78:7b (00:30:05:af:78:7b)
  Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 100
Internet Protocol, Src: 172.16.1.10 (172.16.1.10), Dst: 172.16.1.20 (172.16.1.20)
Internet Control Message Protocol
```

```
Frame 9 (124 bytes on wire, 124 bytes captured)
Ethernet II, Src: Cisco_4b:52:f2 (00:17:5a:4b:52:f2), Dst: Cisco_4b:53:59 (00:17:5a:4b:53:59)
  Destination: Cisco_4b:53:59 (00:17:5a:4b:53:59)
  Source: Cisco_4b:52:f2 (00:17:5a:4b:52:f2)
  Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 1, TTL: 254
PW Ethernet Control Word
Ethernet II, Src: FujitsuS_af:78:7b (00:30:05:af:78:7b), Dst: FujitsuS_8e:5e:4f (00:30:05:8e:5e:4f)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 100
Internet Protocol, Src: 172.16.1.10 (172.16.1.10), Dst: 172.16.1.20 (172.16.1.20)
Internet Control Message Protocol
```

Obr. 5.3 Rozbor rámců při přenosu přes MPLS síť

Komunikace mezi koncovými počítači byla zprostředkována pomocí protokolu ICMP. Rámec přicházející do směrovače PE1obsahuje Ethernetovou hlavičku s cílovou a zdrojovou MAC adresou koncových pracovních stanic (FujitsuS). Tato hlavička dále obsahuje typ rámce, který zapouzdřuje 802.1Q Virtuální LAN s identifikátorem 0x8100 (viz. Obr. 9 - pole TPID). Následuje identifikátor virtuální LAN (poleTCI), kde ID: 100 reprezentuje přenos rámce pro VLAN100. Pokračuje hlavička internetového protokolu obsahující zdrojovou a cílovou IP adresu koncových stanic a identifikuje použitý protokol vyšší vrstvy jako protokol ICMP.

Směrovač PE1 zapouzdří Ethernetovou hlavičku. Na pod-rozhranní Fa0/1.100 je vytvořen tunel pro VLAN100. Směrovač PE1 posílá na rozhranní Fa0/0 nový rámec s Ethernetovou hlavičkou složenou z cílové MAC adresy směrovače P a zdrojové MAC adresy směrovače PE1. Typ přenášených dat je identifikován jako MPLS s identifikátorem 0x8847. Nyní už následuje první MPLS značka. Tunel vytvořený na tomto pod-rozhranní je spojen se směrovačem PE2 přes jeho Loopback adresu 3.3.3.3. Z výpisu *show mpls forwarding-table* zjistíme, jaké značky bude paket používat k dosažení konce tunelu, tedy IP adresy 3.3.3.3/32.

```
PE1#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     2.2.2.2/32       0             Fa0/0      192.168.1.2
17     17            3.3.3.3/32       0             Fa0/0      192.168.1.2
18     Pop Label     192.168.2.0/24   0             Fa0/0      192.168.1.2
19     No Label      l2ckt(100)       46739         Fa0/1.100  point2point
20     Pop Label     192.168.3.0/24   0             Fa0/0      192.168.1.2
21     18            4.4.4.4/32       0             Fa0/0      192.168.1.2
22     No Label      l2ckt(200)       7676          Fa0/1.200  point2point
```

S touto IP adresou je spojena značka 17, tato značka byla přidána jako poslední značka (Top label) k paketu a zajišťuje přepínání až ke zmíněnému cíly. Příznak S: 0 značí, že to není poslední MPLS značka. Výstupní rozhranní pro tuto značku je Fa0/0 směrovače PE1a příští dosažená adresa je 192.168.1.2, což je rozhranní Fa0/1 směrovače P. Za touto značkou následuje značka virtuálního okruhu (Bottom label), tedy značka 19, ta už obsahuje příznak S: 1, označuje poslední MPLS záhlaví. Tato značka je po celou cestu paketu neměnná a definuje nám na jaké virtuální pod-rozhranní se rámec pošle.

Rámec přicházející do směrovače P je rozbalen, je odstraněna Ethernetová hlavička a zkoumají se MPLS značky. Jako první je zkoumána značka 17, ta je ale ihned odstraněna (Pop label), protože se zde uplatňuje funkce PHP. Značka 19 zůstává. Paket je zpět zapouzdřen s novými MAC adresami směrovačů P a PE2, je poslán na rozhranní Fa0/0 a směrován na IP adresu 192.168.2.2 směrovače PE2.

```
P#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     1.1.1.1/32       381280        Fa0/1      192.168.1.1
17     Pop Label     3.3.3.3/32       269034        Fa0/0      192.168.2.2
18     Pop Label     4.4.4.4/32       60342         Se0/1/0    point2point
```

Směrovač PE2 rozbalí rámec. Příchozí značka je 19. Ta se odstraní (No label), protože paket dorazil k cílovému uzlu MPLS sítě. Neoznačený paket je poslán na pod-rozhranní Fa0/0.100 směrovače PE2, kde je definován konec tunelu. Je zpět zapouzdřen do Ethernetové hlavičky a poslán ke koncové stanici PC3.

```
PE2#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     16            1.1.1.1/32       0             Fa0/1      192.168.2.1
17     Pop Label     2.2.2.2/32       0             Fa0/1      192.168.2.1
18     Pop Label     192.168.1.0/24   0             Fa0/1      192.168.2.1
19     No Label      l2ckt(100)       4911          Fa0/0.100  point2point
20     Pop Label     192.168.3.0/24   0             Fa0/1      192.168.2.1
21     18            4.4.4.4/32       0             Fa0/1      192.168.2.1
```

Jelikož pro každý směr existuje jiná LSP (Label Switch Path), ze směrovače PE2 se ICMP paket bude vracet zpět použitím značky 19, ta značí opět virtuální okruh. Dále se přidá značka 16, která identifikuje cílovou IP adresu tunelu což je v tomto případě 1.1.1.1/32. Takto označený rámec dorazí do směrovače P, kde se značka 16 odstraní a paket je směrován přes rozhranní Fa0/1 ke směrovači PE1. Paket přichází do směrovače PE1 pouze se značkou 19, ta se ve směrovači odstraní a paket je směrován na pod-rozhranní Fa0/1.100 a přes přepínač AS3 se dostane až k cílové stanici PC1.

# 6. Frame Relay over MPLS

Frame Relay je vysoce výkonný protokol pro WAN sítě, který operuje na fyzické a linkové vrstvě ISO/OSI modelu. Mezi roky 1970 až 1990 byla nejpoužívanější WAN technologie X.25, byl to velmi populární protokol přepínání paketů. Jeho výhodou bylo velmi spolehlivé spojení přes nespolehlivou infrastrukturu. Protokol Frame Relay vychází právě z X.25 protokolu, který pracoval mimo fyzické a linkové vrstvě také na síťové. Tím pádem musel zaručit detekci chyb a kontrolu provozu. Modernější Frame Relay nabízí spolehlivější spojení než starší technologie. Frame Relay nepoužívá detekci chyb jako X.25. Jednoduše zahodí chybný paket, opravu chyb a kontrolu provozu nechávají na protokolech vyšší vrstvy. Technologie Frame Relay poskytuje také více logických spojení přes jeden fyzický okruh.

Výhodou této novější technologie je cena, každý zákazník má svoji linku připojenou k uzlu Frame Relay, zákazník si tedy nemusí pronajímat drahou linku. Frame Relay má menší režii, tím nezatěžuje zbytečně šířku pásma. Dalšími výhodami jsou lehká implementace, spolehlivost a garantování určité šířky pásma pro virtuální okruh garantovaný poskytovatelem.

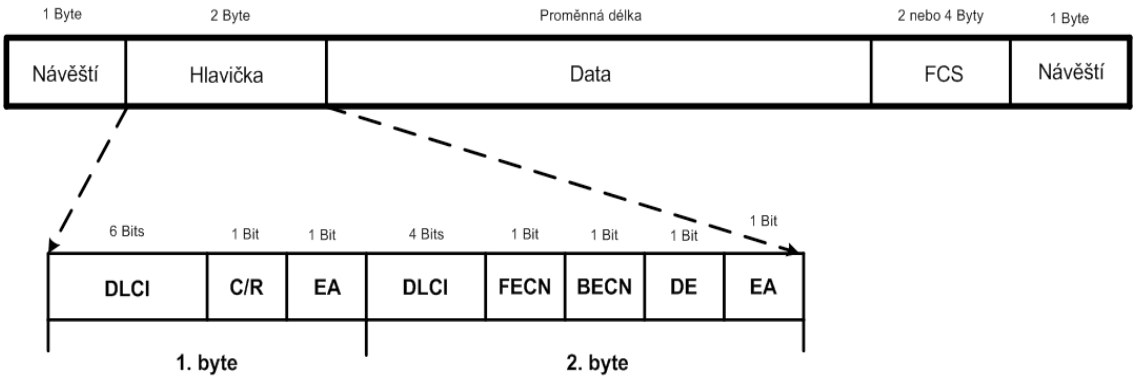
**Frame Relay zapouzdření:**

Návěští: stejná funkce jako u protokolů HDLC a PPP, slouží k ohraničení rámců

Hlavička: je složena ze dvou oktetů, obsahuje 10ti bitové DLCI a stavové bity pro indikaci přetížení a délky hlavičky

Data: datová část paketu, max. délka je 8kB

FCS: kontrolní součet, ověřuje správnost přenesených dat




Obr. 6.0 Zapouzdření Frame Relay rámce

DLCI: Data Link Connection Identifier, 10ti bitový identifikátor virtuálního okruhu, má pouze lokální význam

C/R: Command/Response, stavový bit sloužící pro účely vyšších vrstev

EA: Extended Address, bit uzavírající každý oktet v hlavičce, hodnota 1 značí poslední oktet

FECN, BECN, DE: bity sloužící k řízení toku a indikaci přetížení

## 6.1 Metody Frame Relay over MPLS

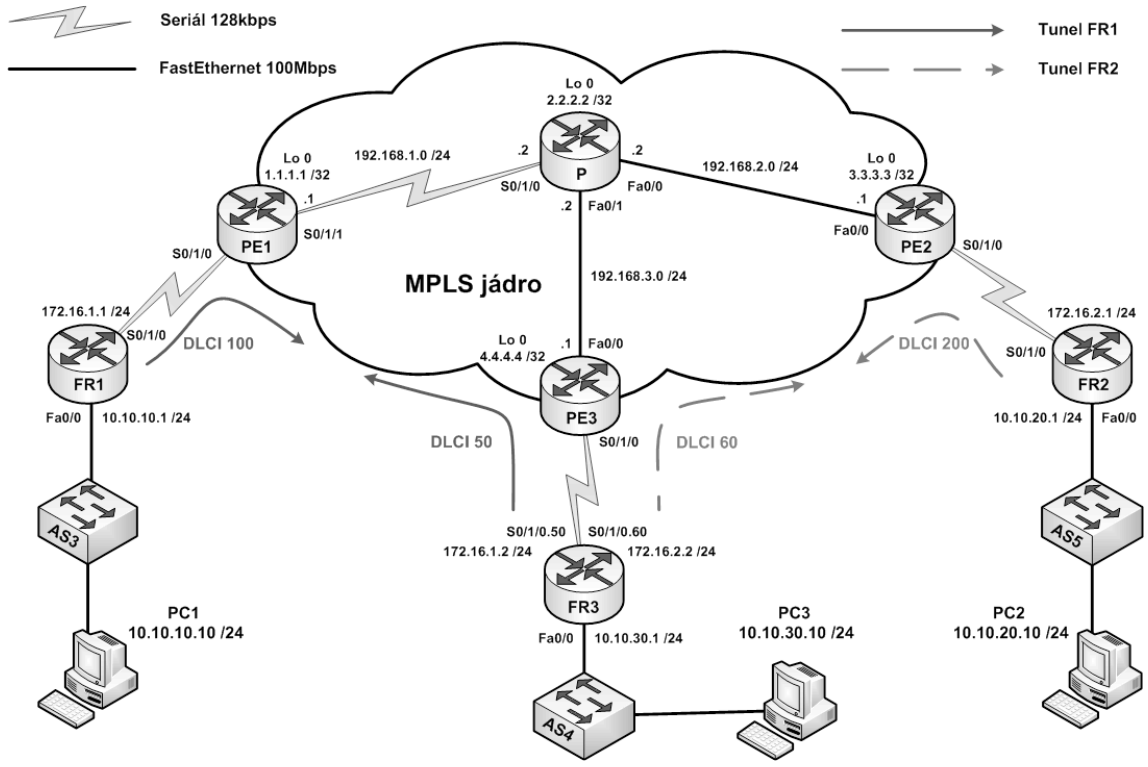
Technologie Frame Relay může být přenášena přes MPLS jádro dvěma způsoby, podobně jako u Ethernetu. Jedná se o DLCI-to-DLCI a port-to-port metody.

U metody DLCI-to-DLCI je jeden virtuální okruh nesen přes jeden tunel. Tím vzniká mapování jedna k jedné, a tudíž můžeme vytvořit samotný tunel pro jednotlivé DLCI. Po příchodu rámce do hraničního směrovače PE, dochází k odstranění hlavičky rámce, přidají se MPLS záhlaví, kontrolní bity FECN, BECN, DE se zkopírují do Control word. Nevýhodou této metody je, že MPLS nepřenáší LMI (Local Management Interface) mezi Frame Relay zákazníky. LMI je ukončeno na hraničních směrovačích. LMI protokol určuje status okruhu. V tomto případě máme dva druhy LMI a to mezi směrovači CE1 – PE1 a PE2 – CE2. Mezi těmito dvojicemi směrovačů nastavujeme zákaznické směrovače jako DTE a hraniční směrovače MPLS jako DCE, kde taky nastavujeme rychlost linky pomocí příkazu *clock rate*.

Port-to-Port metoda může přenášet více virtuálních okruhu přes jediný tunel. Slouží jako trunk přenášející více virtuálních okruhů mezi dvěma PE směrovači. Hraniční směrovače PE používají zapouzdření HDLC pro tuto metodu. V tomto případě se LMI přenáší přes MPLS síť, zákaznické směrovače musí být nastaveny jako DTE a DCE, oba tyto směrovače se podílejí na stavu LMI.

## 6.2 Konfigurace Frame Relay

Jádro MPLS je uspořádáno do topologie hub and spoke, jako hub vystupuje směrovač P a spoke směrovače PE. Pro přenos zákaznických dat je využita metoda DLCI-to-DLCI. Hraniční směrovač PE3 přepíná provoz podle DLCI značek. Mezi zákaznickými směrovači FR3 a FR1 dochází k přepínání DLCI 50 a 100 a mezi směrovači FR3 a FR2 přepínání DLCI 60 a 200. Na směrovači FR3 jsou vytvořena pod-rozhranní S0/1/0.50 pro DLCI 50 a S0/1/0.60 pro DLCI 60. Hraniční směrovač PE3 vytváří tunely ke směrovačům PE1 a PE2. Sériová rozhranní směrovačů PE používají Frame Relay zapouzdření a jsou nastaveny jako DCE, směrovače jsou taky nastaveny pro Frame Relay přepínání. Zákaznické směrovače nastavujeme jako DTE.




Obr. 6.2 Topologie pro přenos Frame Relay přes MPLS jádro

Konfigurace MPLS jádra zde není popsána, jelikož je uvedena v předchozích kapitolách. Cílenou LDP relaci vytvoříme mezi směrovači PE3 – PE1 a PE3 – PE2.

Cílená LDP relace mezi PE3 – PE1:

```
PE3 (config)# mpls ldp neighbor 1.1.1.1 targetted ldp
PE1 (config)# mpls ldp neighbor 4.4.4.4 targetted ldp
```

Nyní nastavíme PE směrovače pro Frame Relay zapouzdření a přepínání, jako typ zařízení zvolíme DCE.

Konfigurace Frame Relay na směrovači PE3:

```
PE3 (config)#frame-relay switching
PE3 (config)# interface s 0/1/0
PE3 (config-if)# encapsulation frame-relay
PE3 (config-if)# frame-relay intf-type dce
PE3 (config-if)# frame-relay lmi-type ansi
PE3 (config-if)# clock rate 128000
PE3 (config-if)# no shutdown
```

Konfigurace se shoduje pro všechny hraniční PE směrovače. Následuje nastavení zákaznických směrovačů FR. Zde není potřeba nastavovat frame relay přepínání, protože směrovače se na přepínání frame relay rámců nepodílí. Na směrovači PE3 vytvoříme již zmíněné pod-rozhranní a přiřadíme jim řádnou DLCI značku, pod-rozhranní jsou nastaveny jako linka bod-bod, tzn. obě pod-rozhranní jsou na rozdílné podsíti. Nastavíme jejich IP adresy.

Konfigurace Frame Relay na směrovači FR3:

```
FR3 (config)# interface s 0/1/0
FR3 (config)# encapsulation frame-relay
FR3 (config-if)# frame-relay lmi-type ansi
FR3 (config-if)# exit
```

```
FR3 (config)# interface s 0/1/0.50 point-to-point
FR3 (config-subif)# ip address 172.16.1.2 255.255.255.0
FR3 (config-subif)# frame-relay interface-dlci 50
FR3 (config-subif)# exit
```

Konfigurace pro pod-rozhranní S 0/1/0.60 je podobná, liší se pouze v přiřazené IP adrese a DLCI. IP adresa je v tomto případě 172.16.2.2 a DLCI je 60. Pod-rozhranní aktivujeme příkazem *no shutdown* na rozhranní S0/1/0.

Poslední krok spočívá ve vytvoření tunelů mezi jednotlivými PE směrovači. Konfigurace je rozdílná oproti předchozím, tunel se nevytváří přímo na rozhranní resp. pod-rozhranní. Je vytvořen v globálním konfiguračním módu. Nejdříve definujeme název tunelu, lokální rozhranní a značku DLCI. Poté se dostaneme do pod-konfiguračního režimu, kde specifikujeme MPLS zapouzdření, výstupní PE směrovač, což je IP adresa Loopback rozhranní a nakonec přiřadíme identifikátor virtuálního okruhu.

Vytvoření L2 tunelu mezi směrovači PE3 – PE1:

```
PE3 (config)# connect FR1 serial0/1/0 50 l2transport
PE3 (config-fr-pw-switching)# mpls l2transport route 1.1.1.1 100

PE1 (config)# connect FR1 serial0/1/0 100 l2transport
PE1 (config-fr-pw-switching)# mpls l2transport route 4.4.4.4 100
```

Podobně vytvoříme tunel mezi směrovači PE3 – PE2. Nyní máme vytvořeny tunely mezi směrovači PE3 – PE1 a PE3 – PE2. Pokud budeme posílat data ze zákaznického směrovače PE3 ke směrovači PE1, bude docházet k přepínání DLCI značek z 50 na 100 a naopak. Pro přenos mezi směrovači PE3 a PE2 jsou využity značky 60 a 200.

Frame Relay mapování na směrovači FR3:

```
FR3#sh frame-relay map
Serial0/1/0.50 (up): point-to-point dlci, dlci 50(0x32,0xC20), broadcast
          status defined, active
Serial0/1/0.60 (up): point-to-point dlci, dlci 60(0x3C,0xCC0), broadcast
          status defined, active
```

Kontrola vytvořeného L2 tunelu mezi směrovač PE3 – PE1:

```
PE3#sh mpls l2transport vc 100 detail
Local interface: Se0/1/0 up, line protocol up, FR DLCI 50 up
  Destination address: 1.1.1.1, VC ID: 100, VC status: up
    Output interface: Fa0/0, imposed label stack {16 21}
    Preferred path: not configured
    Default path: active
    Next hop: 192.168.3.2
  Create time: 01:41:15, last status change time: 01:41:15
  Signaling protocol: LDP, peer 1.1.1.1:0 up
    MPLS VC labels: local 21, remote 21
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 335, send 1404
    byte totals:   receive 25105, send 154237
    packet drops:  receive 0, seq error 0, send 0
```

Přiřadíme IP adresy koncovým stanicím, a vyzkoušíme funkci nyní pomocí příkazu *traceroute*. Tento příkaz nám ukazuje, přes které směrovače paket prochází až do svého cíle.

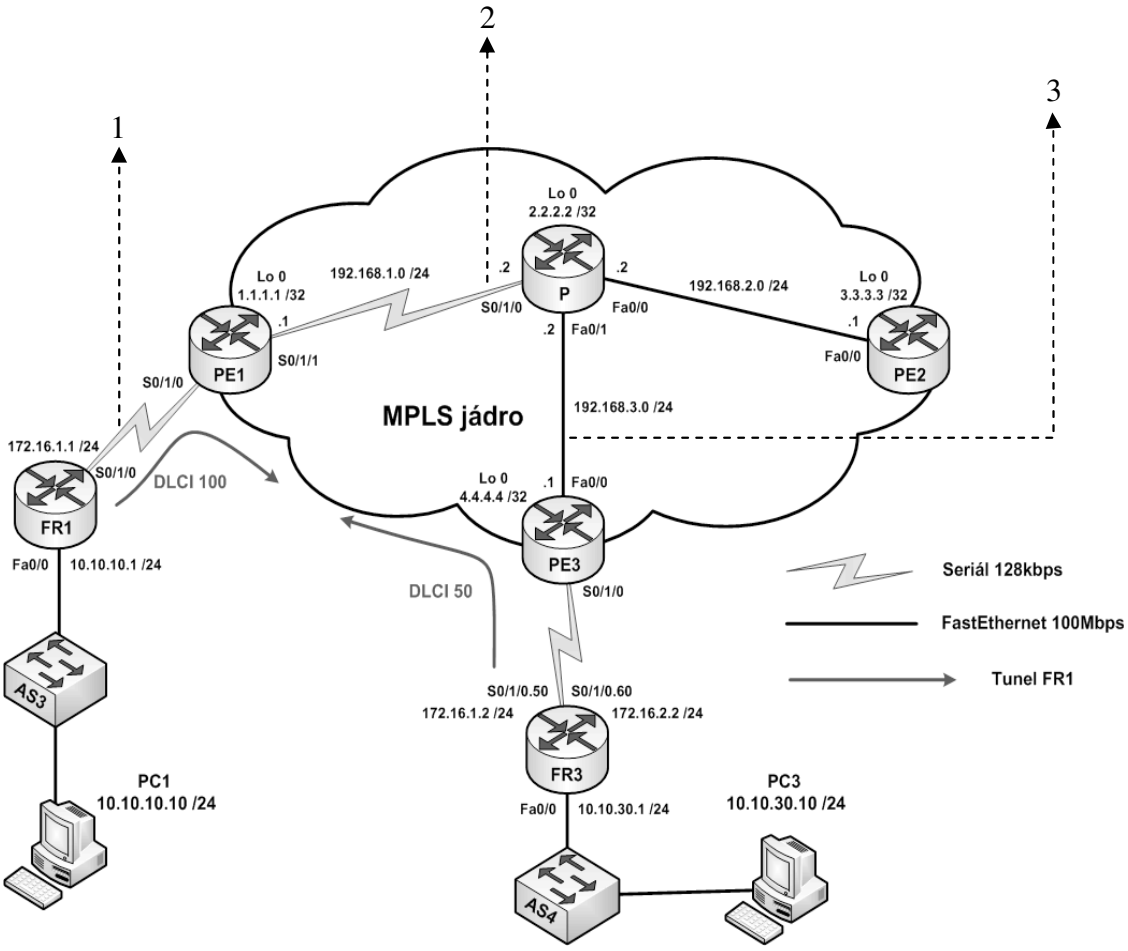
Cesta paketu z pracovní stanice PC1 ke stanici PC3:

```
root@student-desktop:~# traceroute 10.10.30.10
traceroute to 10.10.30.10 (10.10.30.10), 30 hops max, 40 byte packets
 1  10.10.10.1 (10.10.10.1)  1.091 ms  1.266 ms  1.451 ms
 2  172.16.1.2 (172.16.1.2)  30.005 ms  35.161 ms  40.835 ms
 3  10.10.30.10 (10.10.30.10)  53.662 ms  89.072 ms  74.845 ms
```

Příkaz byl proveden na pracovní stanici PC1 s IP adresou 10.10.10.10, cílová IP adresa je PC3 s IP adresou 10.10.30.10. Řádek číslo 1 nám ukazuje, že paket dosáhl své brány s IP adresou 10.10.10.1 na směrovači FR1. Dále paket pokračuje ke směrovači FR3 s IP adresou 172.16.1.2. Zde stojí také za povšimnutí, že paket přestože je transportován pomocí MPLS jádra, se jádro jeví jako neviditelné z pohledu FR směrovačů. Zákaznické směrovače se jeví jako přímo připojené, aniž by věděly, že nějaká MPLS síť mezi nimi figuruje. Poté následuje koncová stanice PC3 s cílovou IP adresou 10.10.30.10.

## 6.2 Zapouzdření Frame Relay rámce přes MPLS síť

V této kapitole je analyzován Frame Relay rámec paketovým analyzátorem Wireshark. Rámec je rozebrán na třech místech topologie. První analýza je provedena mezi zákaznickým směrovačem FR1 a hraničním směrovačem PE1 MPLS sítě. Zde je rozebrán rámec a jeho linkové zapouzdření. Dále je rámec popsán z pohledu MPLS zapouzdření, na směrovači PE1 se přidávají první MPLS záhlaví a podle těchto značek je rámec přepínám ke směrovači P. Ze směrovače P je paket dále přepínán ke koncovému směrovači PE3, kde je ukončen tunel pro Frame Relay okruh, z tohoto směrovače putuje rámec zpět ve Frame Relay zapouzdření ke směrovači FR3.




Obr. 6.3 Frame Relay rámec při přechodu MPLS sítí

Rámec mezi směrovači FR1 a PE1 je zapouzdřen jako Frame Relay, ale Wireshark používá výchozí dekódování pro Frame Relay FRF3.2/CISCO HDLC. Proto vidíme rámec Frame Relay jako HDLC. Pro analýzu rámců je použit protokol ICMP. Jako zdroj byla použita pracovní stanice PC1 s IP adresou 10.10.10.10, cílovou stanicí byla stanice PC3 s IP adresou 10.10.30.10.

Rámec 1: zapouzdření mezi směrovači FR1 a PE1

```
⊞ Frame 388 (104 bytes on wire, 104 bytes captured)
⊞ Cisco HDLC
⊞ Internet Protocol, Src: 10.10.10.10 (10.10.10.10), Dst: 10.10.30.10 (10.10.30.10)
⊞ Internet Control Message Protocol
```

Takto zapouzdřený rámec přichází do směrovače PE1, kde je definovaná LSP ze směrovače PE1 do cílového směrovače PE3. Ve vstupním směrovači PE1 dochází k rozbalení rámce Frame Relay. K paketu je přidán control word, který je u této technologie požadován. Do control word se zkopírují všechny řídící bity z Frame Relay hlavičky. Dále se k paketu přidají MPLS záhlaví, značka 17 zaručuje přepínání paketu ke směrovači PE3.Značka 21 je poslední MPLS značkou protože má nastaven příznakový bit S:1. Tato značka označuje tunel mezi směrovači PE1 a PE3 a je po celou dobu přepínání paketu stejná.

Rámec 2: zapouzdření mezi směrovači PE1 a P

```
⊞ Frame 280 (128 bytes on wire, 128 bytes captured)
⊞ Ethernet II, Src: ca:03:13:a8:00:08 (ca:03:13:a8:00:08), Dst: ca:04:13:a8:00:08 (ca:04:13:a8:00:08)
⊞ MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 0, TTL: 255
⊞ MultiProtocol Label Switching Header, Label: 21, Exp: 0, S: 1, TTL: 255
⊟ PW Frame Relay DLCI Control Word: 0x00000000
    .... 0... = FR FECN: 0
    .... .0.. = FR BECN: 0
    .... ..0. = FR DE bit: 0
    .... ...0 = FR Frame C/R: 0
    00.. .... = Fragmentation: Unfragmented (0)
    ..00 0000 = Length: 0
    Sequence number: 0
⊞ Frame Relay
  Frame relay lapf not yet implemented
⊞ Data (102 bytes)
```

Z výpisu *sh mpls forwarding-table* můžeme vyčíst, že značka 21 je použitá pro tunel 100 mezi směrovači PE1 a PE3. Značka 17 má za cílovou IP adresu Loopback směrovače PE3 což je adresa 4.4.4.4/32, výchozí rozhranní je Se0/1/1 směrovače PE1

Výpis MPLS tabulky ze směrovače PE1:

```
PE1#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     2.2.2.2/32       0          Se 0/1/1    192.168.1.2
17     Pop tag     192.168.2.0/24   0          Se 0/1/1    192.168.1.2
18     Pop tag     192.168.3.0/24   0          Se 0/1/1    192.168.1.2
19     17          4.4.4.4/32       0          Se 0/1/1    192.168.1.2
20     18          3.3.3.3/32       0          Se 0/1/1    192.168.1.2
21                 l2ckt(100)       39663      none        point2point
```

V MPLS síti Wireshark detekuje Frame relay rámce jako Ethernet II, proto rámce musíme dekódovat jako Frame relay DLCI PW. Po příchodu rámce do P směrovače, se podle značky 17 určí další cesta paketu a tato značka se odstraní. Paket je dále přepínán ke směrovači PE3. Směrovač P nezkoumá značku virtuálního okruhu (značka 21) a taky nezkoumá control word.

```
P#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     1.1.1.1/32       381280        Se0/1/0     192.168.1.1
17     Pop Label     4.4.4.4/32       269034        Fa0/1       192.168.3.1
18     Pop Label     3.3.3.3/32       60342         Fa0/0       192.168.2.1
```

Rámec přicházející do směrovače PE3 nese pouze značku virtuální okruhu, značka LSP byla odstraněna ve směrovači P, mezi směrovači P a PE3 dochází k funkci Penultimate hop popping (PHP), poslední přidaná značka je odstraněna ve směrovači P, není potřeba nést tuto značku do cílového směrovače.

Rámec 3: zapouzdření mezi směrovači P a PE3

```
⊞ Frame 1571 (84 bytes on wire, 84 bytes captured)
⊞ Ethernet II, Src: ca:04:04:bc:00:1c (ca:04:04:bc:00:1c), Dst: ca:02:0b:88:00:08 (ca:02:0b:88:00:08)
⊞ MultiProtocol Label Switching Header, Label: 21, Exp: 0, S: 1, TTL: 254
⊞ PW Frame Relay DLCI Control Word: 0x00000000
⊞ Frame Relay
  Frame relay lapf not yet implemented
⊞ Data (62 bytes)
```

Ve směrovači PE3 dochází k odstranění značky virtuálního okruhu. Podle control word je zpět poskládán Frame Relay rámec. Ten je poslán do směrovače FR3.

```
PE3#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     18          3.3.3.3/32       0          Fa0/0      192.168.3.2
17     Pop tag     2.2.2.2/32       0          Fa0/0      192.168.3.2
18     16          1.1.1.1/32       0          Fa0/0      192.168.3.2
19     Pop tag     192.168.2.0/24   0          Fa0/0      192.168.3.2
20     Pop tag     192.168.1.0/24   0          Fa0/0      192.168.3.2
21                 l2ckt(100)       23797      none       point2point
22                 l2ckt(200)       1058       none       point2point
```

Nazpět je paket posílán zase se značkou virtuálního okruhu 21, další přidaná značka je 16, ta se stará o doručení paketu ke směrovači PE1.

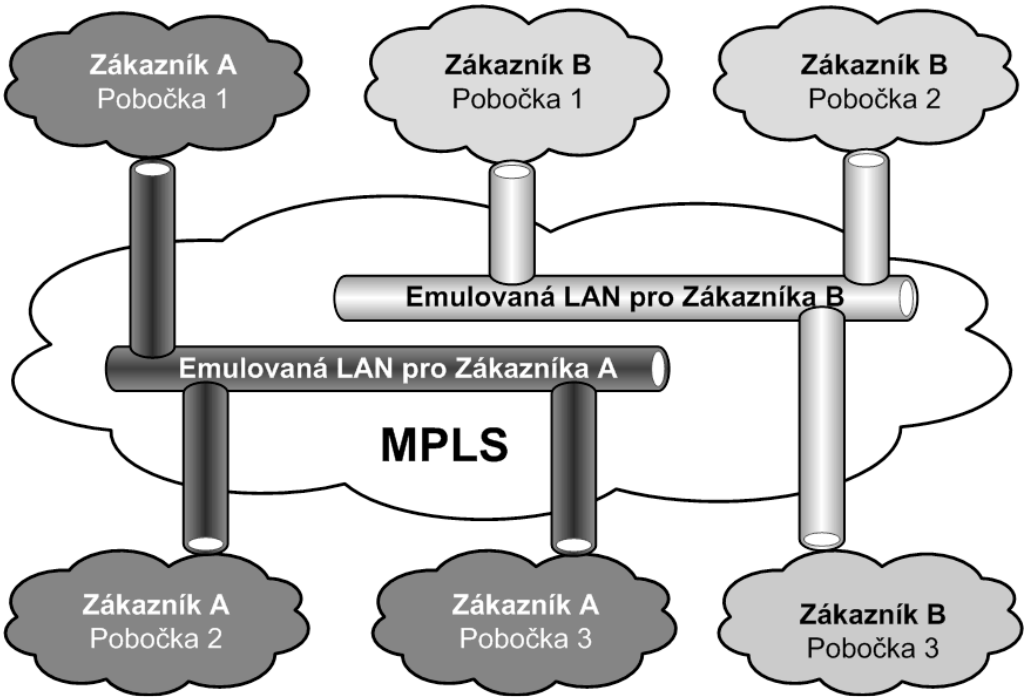
Rozdíl mezi přenosem Frame relay technologie a ostatních protokolů přes MPLS síť je v použití Control word. Ten musí být součástí u technologií Frame Relay a ATM při přenosu přes MPLS síť. Všechny důležité informace zabalené v hlavičce rámce jsou zkopírovány do control word, takto zapouzdřené rámce jsou přeneseny do cílového směrovače, kde se opět složí hlavička Frame Relay nebo ATM rámce.

# 7. Technologie VPLS

Virtuální privátní LAN služba (VPLS) je VPN technologie, umožňující přenos Ethernetových rámců přes MPLS páteřní síť.

Technologie AToM, přenášející rámce linkové vrstvy, využívá spojení typu bod-bod. Toto spojení je dobře využitelné pouze pro sériové linky typu HDLC, PPP, Frame Relay atd. avšak pro Ethernetové segmenty je ve většině případů potřeba využít spojení typu bod-více bodů. Právě technologie VPLS nabízí tuto možnost.

Technologie VPLS emuluje LAN segment a propojuje zákaznické pobočky mezi sebou. Slovo privátní v názvu VPLS označuje, že jednotliví zákazníci jsou od sebe logicky oddělení, jak naznačuje obr. 7.1.



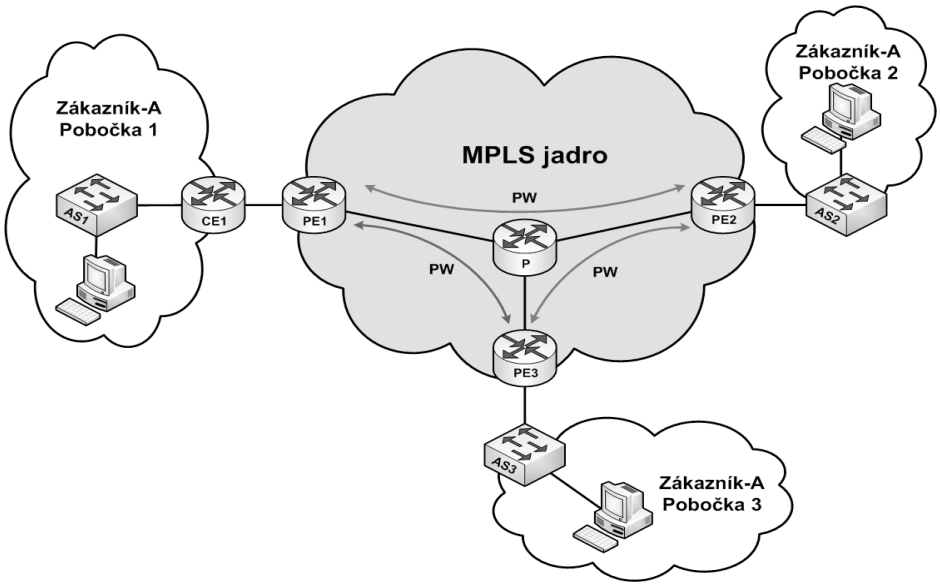

Obr. 7.1 Emulace LAN segmentů pro jednotlivé zákazníky

Primárním účelem VPLS je poskytnout konektivitu mezi geograficky vzdálenými lokacemi přes WAN nebo MAN sítě [4]. Samotná služba VPLS se chová jako L2 přepínač a samozřejmě přebírá i jeho vlastnosti jako je všesměrové a skupinové vysílání, přeposílání Ethernetových rámců pro neznámé cílové MAC adresy, prevence proti smyčkám, dynamické učení MAC adres a jejich vypršení.

## 7.1 Základní princip VPLS

Tato kapitola popisuje chování technologie VPLS, způsob přidávání MPLS záhlaví k Ethernetovým rámcům a samotnou architekturu této služby.

Obr. 7.2 představuje základní topologii této technologie. Stejně jako technologie AToM tak i technologie VPLS vychází ze směrovačů poskytovatele PE, kde vytváříme veškeré tunely a virtuální okruhy mezi jednotlivými směrovači. Všechny PE směrovače, které náleží do jedné VPLS instance musí mít mezi sebou vytvořeny virtuální okruhy ve full-mash topologii, což znamená, že musí být definovány všechny vzdálené PE směrovače náležící do této instance.

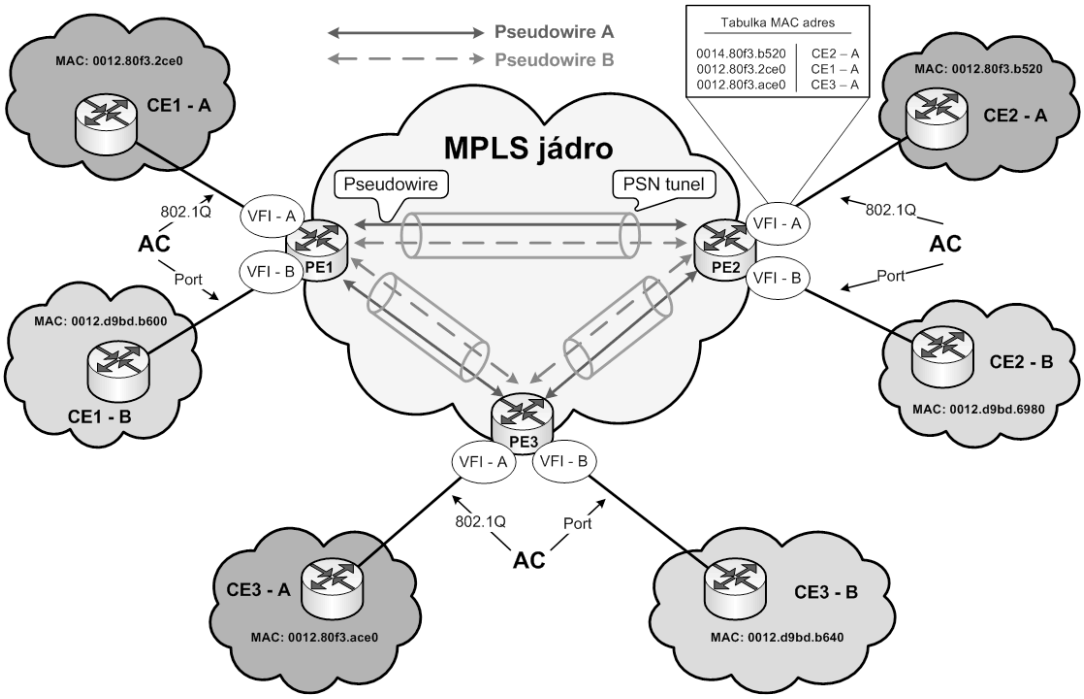



Obr. 7.2 Základní hierarchie VPLS

Pokud PE směrovač příjme rámec s neznámou cílovou MAC adresou, rámec je překopírován a přeposílán na všechny porty které náleží do tohoto segmentu. LAN segment na přepínači může být definován pouze pro porty náležící do stejné VLAN. Dále musíme specifikovat do které VPLS instance, porty nebo VLAN náleží. Rámec s neznámou MAC adresou je potom přeposílán na všechny porty přiřazené k této instanci. Na klasickém Ethernetovém přepínači jsou porty fyzické rozhranní, zatímco u VPLS to můžou být také samotné virtuální okruhy k jinému PE směrovači. Na obr. 7.2 vidíme, že PE směrovače jsou zapojené do VPLS instance nazvané Zákazník-A. Zákazník má tři pobočky připojené k PE směrovačům, které mají mezi sebou definované virtuální okruhy pro přenášení Ethernetových rámců. Každý virtuální okruh je složen ze dvou LSP, každý pro jeden směr.

### 7.1.1. Komponenty pro VPLS

Komponenty v tomto smyslu slova znamenají jednotlivé části, které jsou nezbytné pro správnou funkci VPLS.




Obr. 7.3 Technologie VPLS pro zákazníky A (802.1Q mód) a B (Port mód)

Na obr. 7.3 je zobrazena topologie pro VPLS technologii, je složena z MPLS jádra, které obsahuje tři PE směrovače. Směrovače P nejsou v tomto příkladu uvedeny pro zjednodušení a přehlednost. Do směrovačů PE jsou připojeny zákaznické sítě CEx - A a CEx - B, každá z nich má 3 různé lokace. Nejdříve se zaměříme na MPLS jádro. Mezi dvěma PE směrovači je sestaven PSN tunel, tento tunel se podílí na přenosu provozu, v tomto případě Ethenetového. Tunel slouží k přenosu jednoho nebo více virtuálních okruhů, nebo chcete-li pseudowire. V tomto případě jsou vytvořeny dva virtuální okruhy (VC – virtual circuit), každý pro jednoho zákazníka. Virtuální okruh propojuje dva připojené okruhy (AC – attachment circuit) mezi sebou. Tedy propojuje mezi sebou dvě zákaznické sítě.

Každý PE směrovač obsahuje tzv. VFI entitu (Virtual Forwarding Instance), která definuje jednotlivé členy ve VPLS doméně. To znamená, že do VPLS domény zákazníka A patří všechny rozhranní PE směrovače, přiřazené k této instanci. Obdobné je to i v případě zákazníka B. Dále každý PE směrovač obsahuje VSI entitu (Virtual Switching Instance), ta se učí vzdálené MAC adresy fyzických rozhranní a virtuálních okruhů, je také odpovědna za správné posílání zákaznického provozu ke správným koncovým uzlům. V neposlední řadě se také snaží udržovat VPLS doménu ve stavu bez smyček. Pro tento stav používá VPLS funkci zvanou split horizon, metoda díky níž je zakázáno posílání směrovacích cest zpět na rozhranní ze kterého informace přišli.

Do každého PE směrovače jsou připojeny zákaznické sítě přes připojený okruh. AC je okruh linkové vrstvy ve spojení typu bod-bod. Okruh propojuje zákaznické zařízení (CE) se zařízeními poskytovatele (PE). VPLS podporuje tři typy těchto okruhů pro Ethernet. Port mód, 802.1Q mód a Dot1q tunel mód.

Rozhranní pracující v Port módu akceptuje pouze neoznačené Ethernetové rámce. Směrovač PE příjme Ethernetový rámec a podle cílové MAC adresy zjistí, jakým virtuálním okruhem jej pošle ke svému cíly. Mód 802.1Q neboli trunk mód spočívá v tom, že linka mezi zákaznickým zařízením a zařízením poskytovatele je nakonfigurována jako trunk, linka může přenášet více označených rámců najednou a spolu s nimi taky nativní VLAN. Podle označení VLAN vybere PE směrovač, který virtuální okruh použít ke koncovému uzlu. Poslední typ Dot1q tunel zapouzdřuje 802.1Q trunk do dalšího trunku. Každý rámec je tedy označkován dvakrát, vnitřní 802.1Q hlavička obsahuje VLAN ID, který je vybrán zákazníkem a vnější 802.1Q hlavička obsahuje VLAN ID označenou poskytovatelem pro zákazníka. Zjednodušeně můžeme říct, že pro přenos přes jádro poskytovatele je zákaznické VLAN ID zapouzdřeno do VLAN ID poskytovatele.

### 7.1.2 Zapouzdření Ethernetových rámců

Transport Ethernetových rámců se provádí stejným způsobem jako u modelu AToM. K Ethernetovému rámci jsou přidávány postupně dvě MPLS záhlaví. Jako první se přidá značka virtuálního okruhu (VC značka), tato značka se také nazývá Bottom značka. Zdrojový PE směrovač označí rámec touto značkou podle cíle, který chce rámec dosáhnout. Rámec dále směřuje přes virtuální okruh označený touto značkou, cílový PE směrovač dále zkoumá tuto VC značku a podle ní určí, na který připojený okruh (AC) pošle “čistý“ rámec. Tato značka se po dobu přenosu nemění. Dále se k rámci přidává v pořadí druhá značka, nazývá se značka tunelu,

nebo taky Top značka. Tato značka identifikuje tunel neboli cestu podle značek (LSP), ke které rámec náleží. Tyto značky se mění na každém P směrovači podle cesty k cílovému PE směrovači.

Pokud je rámec před příchodem do PE směrovače označen určitým VLAN ID, tato značka je odstraněna, před tím než je rámec posílán do MPLS sítě. Po příchodu rámce do cílového PE směrovače, je rámec zkoumán podle MAC tabulky a podle toho se k němu znovu přiřadí shodné VLAN ID a je poslán ke správnému připojenému okruhu.

## 7.2 Základní konfigurace VPLS

Základ VPLS technologie vychází z MPLS. Celá konfigurace MPLS je popsána v kapitole 2.2 Konfigurace MPLS jádra. Nejprve musíme dosáhnout konektivity mezi všemi Loopback rozhranními všech PE směrovačů, toho dosáhneme nasazením interního směrovacího protokolu. Dále je zapotřebí zapnout protokol LDP pro distribuci značek. V tomto případě nejprve nastavíme lokální sousedství mezi sousedními směrovači.

```
Router (config)# mpls label protokol ldp
Router (config)# mpls ldp router-id <rozhranní> force
```

Pokud máme lokální LDP relaci mezi směrovači poskytovatele platnou, můžeme začít definovat VPLS instanci.

```
Router(config)# l2 vfi <jméno> manual
```

Posledním uvedeným příkazem definujeme VFI instanci linkové vrstvy, jméno této instance se musí shodovat na všech PE směrovačích patřících do jedné instance.

Dále musíme definovat unikátní identifikaci VPN pro tuto VFI instanci. VPN ID identifikuje virtuální okruh, který spojuje všechny PE směrovače této VPLS instance. Musí být shodné na všech PE směrovačích.

```
Router(config-vfi)# vpn id <číslo>
```

Cílené LDP relace navazujeme po vytvoření VFI a určíme, které směrovače se budou podílet v této instanci. Všechny nadefinované PE směrovače vytvoří cílenou LDP relaci mezi sebou ve full-mash topologii.

```
Router(config-vfi)# neighbor <ID vzdáleného PE> encapsulation
                    mpls
```

Nyní je nastavení VFI instance hotova. V posledním kroku musí být tato instance přiřazena určitému rozhranní, aby se mohly vytvořit tunely k cílovým PE směrovačům definovaných v předchozím kroku.

```
Router(config-if)# xconnect vfi <jméno>
```

Příkaz *xconnect* musí být vždy spjat s určitou virtuální LAN sítí ať už se jedné o port mód, 802.1Q mód nebo Dot1Q tunel mód.

Ověření VPLS činnosti:

```
Router # show vfi <jméno>
```

Příkaz ověřuje stav VFI instance stavovými slovy up/down, zobrazuje lokální připojený okruh a sousedy, definované pro tuto instanci.

Zadáním příkazu níže můžeme zjistit, jaké lokální LDP relace jsou navázány mezi sousedními a vzdálenými LDP sousedy.

```
Router # show mpls ldp neighbor
```

Tento příkaz ověřuje existenci virtuálních okruhů přiřazených k instanci. Dále můžeme zkoumat více do hloubky příkazem:

```
Router # show mpls l2transport summary
Router # show mpls l2transport vc <číslo> detail
```

Zde zjistíme k jaké instanci virtuální okruh (VPN ID) patří, jeho status, cílovou adresu, použité značky.

## 7.3 Tunelování protokolů druhé vrstvy

Jelikož se VPLS chová jako virtuální přepínač druhé vrstvy, je nezbytné, aby podporoval také ostatní služby, které využívají fyzické přepínače. Pro větší ethernetové segmenty je samozřejmostí využívat protokoly jako STP, VTP a CDP, což jsou protokoly, které samotným administrátorům usnadňují práci.

Spanning Tree Protokol (STP) udržuje ethernetový segment bez smyček, tím že vypíná z provozu redundantní rozhranní. STP na fyzické topologii, která může obsahovat smyčky, vytvoří virtuální topologii bez smyček. Jak už je z názvu patrné, vychází se z topologie stromu, kde definujeme hlavní přepínač jako kořen (root).

VPLS standardně neposílá datové jednotky protokolu STP přes MPLS poskytovatele, avšak můžeme tuto funkci zapnout příkazem na určitém rozhranní.

```
Router(config-if)# l2protocol-tunel stp
```

Stejná situace je s protokolem Cisco Discovery Protokol (CDP). Tento protokol slouží pro zobrazení přímo připojených zařízení. Protokol se hojně využívá ke kontrole síťových map. Pokud nám mapa chybí, můžeme přes tento protokol vyhledat připojená zařízení a zjistit další informace, jako je použitá platforma, typ softwaru, IP adresy pro vzdálený přístup a další. V tomto případě uvidí zákaznické zařízení přímo zařízení, jež je připojeno přes MPLS poskytovatele. Tunelovaní protokolu CDP zajistíme příkazem na obou PE směrovačích.

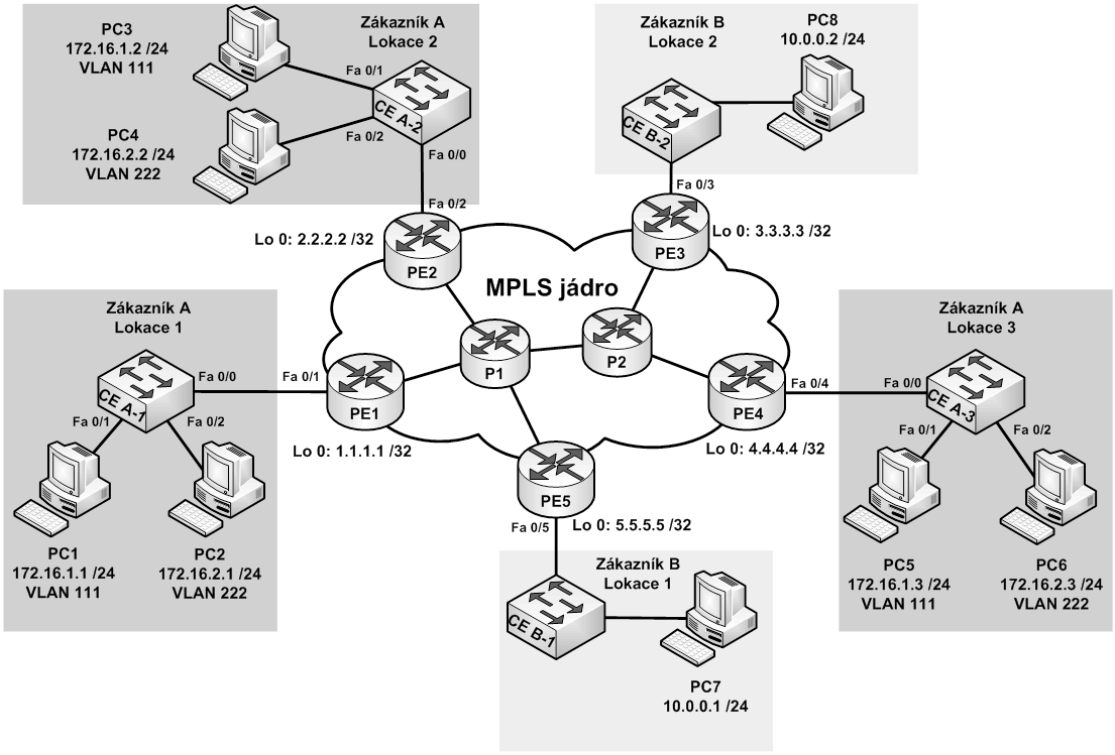
```
Router(config-if)# l2protocol-tunel cdp
```

V poslední řadě zde máme VLAN Trunking Protokol (VTP), který usnadňuje práci s VLAN. Přenáší informace o VLAN mezi přepínači. Tímto protokolem můžeme jednoduše vytvářet, mazat, přejmenovávat VLAN uvnitř VTP domény. Tunelováním tohoto protokolu začnou kontrolní pakety procházet přes MPLS aniž by se směrovače PE na tomto přenose podílely.

```
Router(config-if)# l2protocol-tunel vtp
```

## 7.4 Realizace VPLS

Pro samotnou realizaci technologie jsem navrhl topologii pro dva zákazníky, obr. 7.4 zobrazuje MPLS jádro, které je složeno z pěti hraničních PE směrovačů. Do směrovačů PE1, PE2 a PE4 jsou připojeny okruhy zákazníka A. Zákazník A má celkem tři lokace ve kterých se nacházejí dvě VLAN a to VLAN111 a VLAN222. Proto zde budeme vycházet z typu připojených okruhu 802.1Q. Mezi zákaznickými přepínači a směrovači poskytovatele musí být linka nastavena jako trunk, která bude přenášet obě VLAN. Pro každou VLAN bude definovaný samotný virtuální okruh.




Obr. 7.4 Realizace VPLS pro dvě zákaznické sítě

Zákazník B využívá dvě lokace, které jsou připojeny do směrovačů PE3 a PE5. Ethernetové rámce v tomto případě nejsou značkovány VLAN ID, proto zde použijeme připojené okruhy v port módu.

Základní konfigurace MPLS jádra je popsaná v kapitole 2.2 Konfigurace MPLS jádra. V první řadě musí být dosažitelné všechny Loopback rozhranní mezi sebou. Jakmile jsou adresy Loopback rozhranní jednotlivých PE směrovačů přidány do směrovacích tabulek k propagaci k dalším směrovačům poskytovatele, měla by vzniknout plná konektivita PE směrovačů přes tyto Loopback rozhranní. Loopback rozhranní se používají pro cílené LDP relace, které jsou nezbytné pro sestavení tunelu a vytvoření virtuálních okruhů.

Nastavení Loopback rozhranní pro směrovač PE1:

```
PE1(config)# interface loopback 0
PE1(config-if)# ip address 1.1.1.1 255.255.255.255
```

Loopback rozhranní jsou automaticky funční bez použití příkazu *no shutdown*. Podle obr. 7.4 nastavíme zbývající Loopback rozhranní ostatních PE směrovačů.

Dále pokračujeme spuštěním LDP protokolu. Nejprve vytvoříme lokální sousedství mezi přímo připojené směrovače poskytovatele. Tyto si vzájemně vymění svoje lokální značky.

Nastavení LDP protokolu:

```
PE1(config)# mpls label protokol ldp
PE1(config)# mpls ldp router-id loopback 0 force
```

První příkaz spustí protokol LDP na směrovači. Druhý příkaz definuje jako identifikaci směrovače rozhranní Loopback 0. Příznak *force* donutí změnit identifikaci směrovače na toto rozhranní.

Nyní přejdeme k samotnému nastavení VLPS instance. Nezapomeňme, že zákazník A využívá dvě VLAN pojmenované VLAN111 a VLAN222. Proto musíme pro obě virtuální LAN sítě vytvořit rozdílnou instanci a rozdílný virtuální okruh (VPN ID). Obě instance ale budou využívat shodné vzdálené PE směrovače, v případě směrovače PE1 budou cílení LDP sousedé směrovače PE2 a PE4 pro obě VPLS instance.

Vytvoření VPLS instance na směrovači PE1 pro VLAN111:

```
PE1(config)# l2 vfi zakaznik-A-111 manual
PE1(config-vfi)# vpn id 111
PE1(config-vfi)# neighbor 2.2.2.2 encapsulation mpls
PE1(config-vfi)# neighbor 4.4.4.4 encapsulation mpls
```

Vytvoření VPLS instance na směrovači PE1 pro VLAN222:

```
PE1(config)# l2 vfi zakaznik-A-222 manual
PE1(config-vfi)# vpn id 222
PE1(config-vfi)# neighbor 2.2.2.2 encapsulation mpls
PE1(config-vfi)# neighbor 4.4.4.4 encapsulation mpls
```

Takto vytvořené VPLS instance nyní musíme přiřadit k rozhranní, jelikož používáme 802.1Q mód, v tomto případě musíme vytvořit na směrovači rozhranní VLAN111 a VLAN222.

Vytvoření VLAN rozhranní:

```
PE1(config)# interface vlan 111
PE1(config-if)# no shutdown

PE1(config)# interface vlan 222
PE1(config-if)# no shutdown
```

V posledním kroku přiřadíme VPLS instanci *zakaznik-A-111* k rozhranní *vlan 111* a instanci *zakaznik-A-222* k rozhranní *vlan 222*.

```
PE1(config)# vlan 111
PE1(config-if)# xconnect vfi zakaznik-A-111

PE1(config)# vlan 222
PE1(config-if)# xconnect vfi zakaznik-A-222
```

Pokud provedeme obdobnou konfiguraci na ostatních PE směrovačích náležících do těchto instancí, tzn. směrovače PE2 a PE4, vzniknou mezi všemi směrovači těchto dvou instancí full mash virtuální okruhy. Konfigurace je shodná pro všechny tyto PE směrovače až na definování vzdálených PE směrovačů. Směrovač PE1 používá cílenou LDP relaci se směrovači PE2 a PE4, tzn. adresy 2.2.2.2 a 4.4.4.4. Směrovač PE2 sestavuje tyto relace se směrovači PE1 a PE4, tzn. adresy 1.1.1.1 a 4.4.4.4 a konečně směrovač PE4 využívá jako cílené LDP sousedy směrovače PE1 a PE2 tedy adresy 1.1.1.1 a 2.2.2.2.

Pro ověření správně nakonfigurovaných VPLS instancí můžeme využít následující příkazy. Po zadání prvních dvou příkazů zjistíme, jestli jsou VPLS instance ve stavu up nebo down. Třetí příkaz nám zobrazí všechny LDP relace sestavené mezi směrovači poskytovatele, tedy zobrazí jak lokální tak cílené LDP relace.

```
PE1 # show vfi zakaznik-A-111
PE1 # show vfi zakaznik-A-222
PE1 # show mpls ldp neighbor
```

Pokud jsou VPLS instance ověřeny a jsou funkční, je třeba nastavit linku mezi směrovačem poskytovatele a přepínačem zákazníka jako trunk, linka tedy bude moci přenášet jak VLAN111 tak i VLAN222. Nejdříve nastavíme stranu poskytovatele. Jelikož budeme přenášet dvě virtuální LAN sítě, je potřeba rozdělit rozhranní na PE směrovači na dvě pod-rozhranní. V případě směrovače PE1 se jedná o rozhranní Fa0/1. Toto rozhranní rozdělíme na dvě pod-rozhranní Fa0/1.111 a Fa0/1.222 a zapouzdříme jako dot1q.

Nastavení trunk linky na PE směrovači:

```
PE1(config)# interface fa0/1.111
PE1(config-subif)# encapsulation dot1q 111

PE1(config)# interface fa0/1.222
PE1(config-subif)# encapsulation dot1q 222

PE1(config)# interface fa0/1
PE1(config-if)# no shutdown
```

Strana poskytovatele by mněla být hotová. Nyní se zaměříme na stranu zákazníka, tedy na přepínač.

Vytvoření VLAN:

```
CE A-1 (config) # interface vlan 111
CE A-1 (config-if) # no shutdown
CE A-1 (config) # interface vlan 222
CE A-1 (config-if) # no shutdown
```

Nastavení trunk linky na CE přepínači:

```
CE A-1 (config) # interface fa0/0
CE A-1 (config-if) # switchport mode trunk
CE A-1 (config-if) # switchport trunk allowed add 111
CE A-1 (config-if) # switchport trunk allowed add 222
CE A-1 (config-if) # no shutdown
```

V tomto stavu přenáší linka mezi směrovačem poskytovatele a přepínačem zákazníka požadované VLAN 111 a 222. V posledním bodě přiřadíme koncová zařízení do správné virtuální sítě.

Nastavení přístupových rozhranní pro PC1:

```
CE A-1 (config) # interface fa0/1
CE A-1 (config-if) # switchport mode access
CE A-1 (config-if) # switchport access vlan 111
```

Nastavení přístupových rozhranní pro PC2:

```
CE A-1 (config) # interface fa0/2
CE A-1 (config-if) # switchport mode access
CE A-1 (config-if) # switchport access vlan 222
```

Tím pádem je konfigurace pro zákazníka A hotova. Všechny koncové stanice umístněné u zákazníka A by měly mít konektivitu v rámci určité VLAN sítě.

Stejným způsobem se provádí konfigurace zákazníka B, s tím rozdílem, že koncové stanice zákazníka komunikují v rámci nativní virtuální sítě což je VLAN 1. Ethernetové rámce tedy nejsou nijak značkovány, jsou k nim pouze přidány MPLS záhlaví a jsou směřovány k cílovému uzlu. Není tedy potřeba konfigurovat trunk linku mezi směrovačem a přepínačem. VPLS pracuje v port módu.

Vytvoření VPLS instance na směrovači PE3:

```
PE3(config)# l2 vfi zakaznik-B manual
PE3(config-vfi)# vpn id 10
PE3(config-vfi)# neighbor 5.5.5.5 encapsulation mpls
```

Vytvořili jsme VPLS instanci s názvem *zakaznik-B*. Virtuální okruh pro tuto instanci nese *VPN ID 10*. Zákazník B má pouze dvě lokace tedy každý PE směrovač zákazníka B má pouze jednoho LDP souseda. V případě směrovače PE3 se jedná o cíleného souseda PE5 s adresou 5.5.5.5 a soused pro směrovač PE5 je adresa 3.3.3.3, což je Loopback adresa směrovače PE3.

Jakákoliv VPLS instance musí být spojena s virtuální sítí. Musíme tedy na směrovačích PE vytvořit VLAN. Do této VLAN poté přiřadíme rozhranní PE směrovače, jež je zapojeno k zákaznické síti. V případě lokace 2 zákazníka B se jedná o rozhranní směrovače PE3 Fa0/3 a v případě lokace 1 jde o rozhranní Fa0/5 směrovače PE5.

Vytvoření VLAN na směrovači PE3:

```
PE3(config)# interface vlan 10
PE3(config-vlan)# no shutdown
```

Přiřazení rozhranní k VLAN 10:

```
PE3(config)# interface fa 0/3
PE3(config-if)# switchport mode access
PE3(config-if)# switchport access vlan 10
```

Rozhranní Fa0/3 je přiřazeno do virtuální sítě VLAN10, posledním krokem zůstává vytvoření tunelu v této virtuální síti.

```
PE3(config)# interface vlan 10
PE3(config-if)# xconnect vfi zákazník-B
```

Stejnou konfiguraci provedeme pro směrovač PE5. Poté co tuto konfiguraci dokončíme, realizace VPLS instancí by mněla být hotova pro oba zákazníky.

V tomto příkladu jsme si uvedli dva typy módu pro VPLS, zkráceně zde uvedu také třetí typ, a to Dot1q tunel. Jedná se o zapouzdření zákaznických VLAN do VLAN poskytovatele, tedy musí být vytvořen VLAN tunel. Postup v případě tohoto módu je shodný s port módem. Jediný rozdíl je v tom, že fyzické rozhranní pracuje v módu *dot1q-tunel* namísto *access.* Dále je uvedena konfigurace fyzického rozhranní pro VPLS v tomto módu. Vytvoření VPLS instancí se nijak neliší od předchozích dvou případů, proto není dále uvedena.

Vytvoření VLAN pro Dot1q tunel:

```
Router(config)# interface vlan <název>
Router(config-if)# no shutdown
```

Přiřazení módu k rozhranní:

```
Router(config)# interface <typ> < číslo>
Router(config-if)# switchport mode dot1q-tunel
Router(config-if)# switchport access vlan <název>
```

Vytvoření tunelu:

```
Router(config)# interface vlan  <název>
Router(config-if)# xconnect vfi <jméno>
```

## 7.5 Hierarchická VPLS

Hierarchický model VPLS představuje model, kdy směrovače PE nejsou dále připojeny přímo k zákaznickým sítím. Na obr. 7.5 je model H-VPLS zobrazen. Můžeme si zde všimnout, že mezi MPLS jádrem a zákaznickými sítěmi je připojena další vrstva a to vrstva přístupová. Tento koncept je lépe škálovatelný, pokud jsou lokace zákazníka geograficky odděleny na větší vzdálenost. Přidáním další vrstvy můžeme zaručit lepší spolehlivost a nižší režii při sestavování virtuálních okruhů, jelikož full mash topologii virtuálních okruhu je nyní nutná pouze v MPLS jádru, ne v přístupové vrstvě.

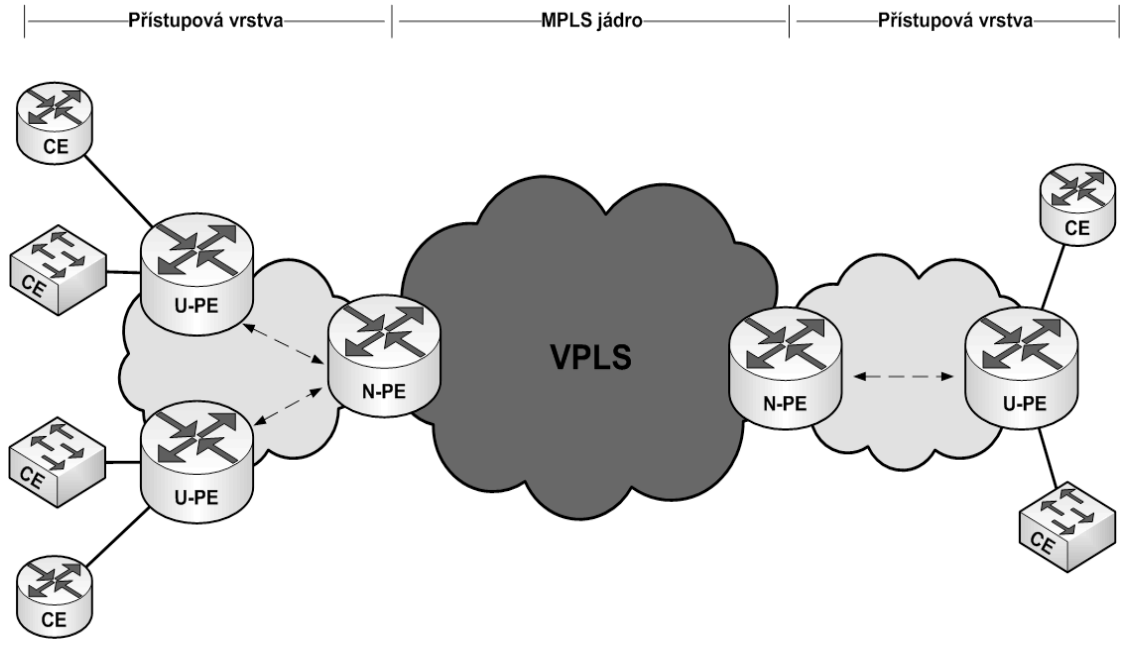
Model H-VPLS může pracovat se dvěma typy přístupových sítí:

- H-VPLS s Dot1q tunelováním
- H-VPLS s MPLS

V hierarchickém modelu VPLS se vyskytují směrovače typu N-PE a U-PE. Směrovače N-PE (Network-Provider Edge) jsou směrovače umístněné mezi MPLS jádrem a přístupovou síť. Zatímco U-PE (User-Provider Edge) jsou směrovače pracující mezi přístupovou vrstvou a sítí zákazníka. Směrovače U-PE přebírají některé funkce směrovačů PE, které byly přítomny v klasické VPLS technologii. Jsou to funkce jako replikace paketů a dynamické učení MAC adres.

Replikace paketů může mít velký dopad na výpočetní výkon směrovače a jeho paměť. Proto pokud vzrůstá počet směrovačů poskytovatele, roste i počet paketů, které potřebují být kopírovány ke koncovým uzlům poskytovatele. Jedná se o všesměrové, skupinové vysílání ale také provoz ARP protokolu, kdy neznáme cílovou MAC adresu koncového uživatele. V této hierarchii přebírá tuto funkci U-PE směrovače aby nedocházelo ke zbytečnému zatěžování jádra VPLS, tedy směrovačů N-PE.

K přístupovým směrovačům poskytovatele U-PE jsou připojeny zařízení zákazníka CE. Mezi směrovači N-PE a U-PE může být zapojena jedna linka. Pokud chceme zaručit redundanci a tím zajistit spolehlivost přístupové sítě, můžou být směrovače U-PE zapojeny k více směrovačům N-PE přes redundantní virtuální okruhy nebo další Dot1q tunely. Tato metoda je známá jako multihoming. V tomto případě použití metody split horizon, pro zajištění stavu sítě bez smyček, není vhodná. Zato musí být povoleno tunelování protokolu STP mezi směrovači U-PE a N-PE. [5]



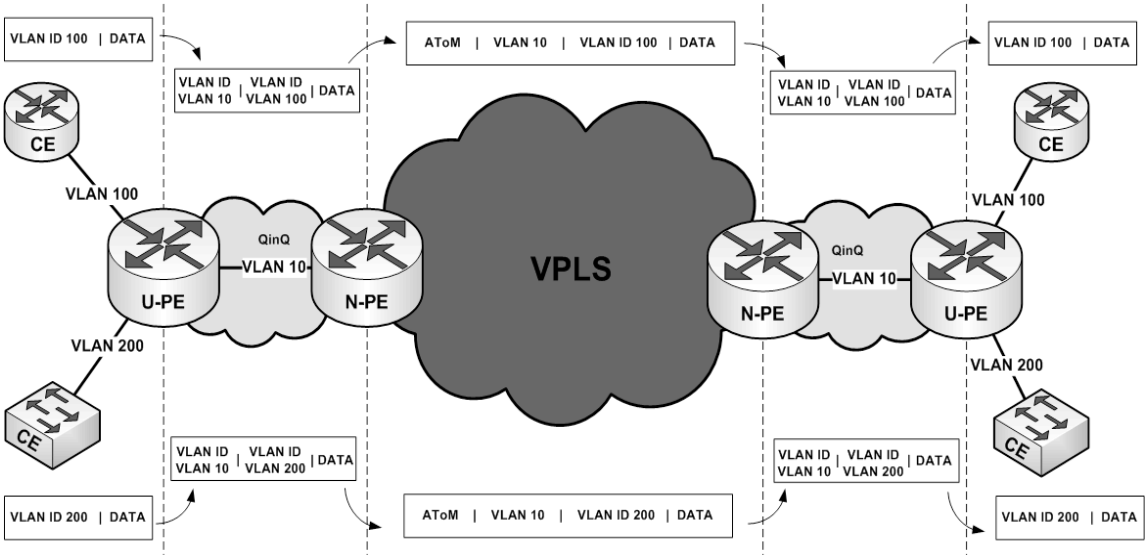

Obr. 7.5 Hierarchický model technologie VPLS

### 7.5.1 H-VPLS s přístupovou vrstvou Dot1q tunel

Pokud přístupovou vrstvu tvoří tunely zapouzdřené do 802.1Q, provoz jednotlivého zákazníkaje zapouzdřen dvakrát. Zkráceně se tento případ nazývá QinQ. Na obr 7.6 je zobrazen průběh tohoto zapouzdření.

Zařízení zákazníka generuje provoz zapouzdřený do hlaviček s VLAN ID 100 a VLAN ID 200. Pokud dojde takový rámec do směrovače U-PE, směrovač zapouzdří tento již

označený rámec do nové hlavičky a to VLAN 10. K takto označenému rámci jsou přidány dvě MPLS záhlaví, MPLS značkování je zprostředkováno směrovači N-PE. Poté jsou tyto dvojitě zapouzdřené rámce přenášeny přes MPLS jádro k cílovému N-PE směrovači, kde dochází k odstranění MPLS záhlaví. Na konečném směrovači U-PE je také odstraněna hlavička poskytovatele VLAN 10. Směrovač U-PE zjistí, kterému připojenému okruhu provoz náleží, buď pro VLAN 100 nebo VLAN 200.



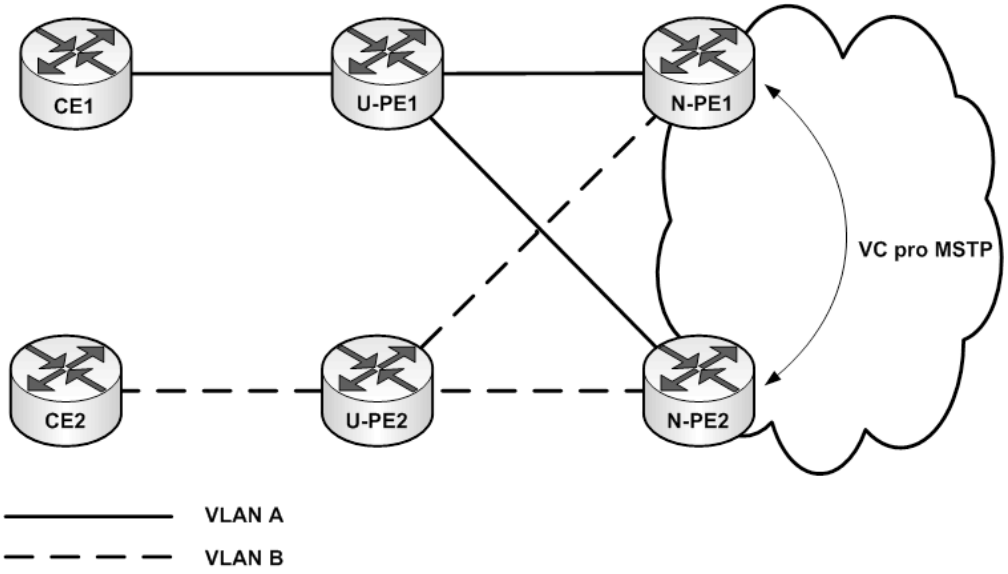

Obr. 7.6 Přístupová vrstva využívající Dot1q tunel

Konfigurace takového zapouzdření je zobrazena níže. Takto musí být nastaveny rozhranní obou směrovačů U-PE a N-PE mezi nimiž linka je. Na N-PE směrovači je vytvořena VPLS instance pro tuto VLAN 10.

Vytvoření Dot1q tunelu mezi U-PE a N-PE směrovači:

```
x-PE(config)#vlan 10
x-PE(config-if)#interface <typ> < číslo>
x-PE(config-if)# switchport access vlan 10
x-PE(config-if)# switchport mode dot1q-tunnel
```

Redundance na přístupové vrstvě by měla být vždy zajištěna pro větší spolehlivost sítě. V tomto případě redundanci mezi U-PE a N-PE směrovači zajišťuje MSTP (Multiple STP). Protokol pro zaručení stavu bez smyček pro více VLAN instancí. Virtuální okruh mezi N-PE směrovači je pouze pro přenos datových jednotek protokolu MSTP. Tento virtuální okruh je vždy funkční a MSTP přes něj rozhoduje, kterou cestu mezi směrovači U-PE a N-PE bude blokovat. Pokud je primární cesta nefunkční, MSTP odblokuje záložní cestu.

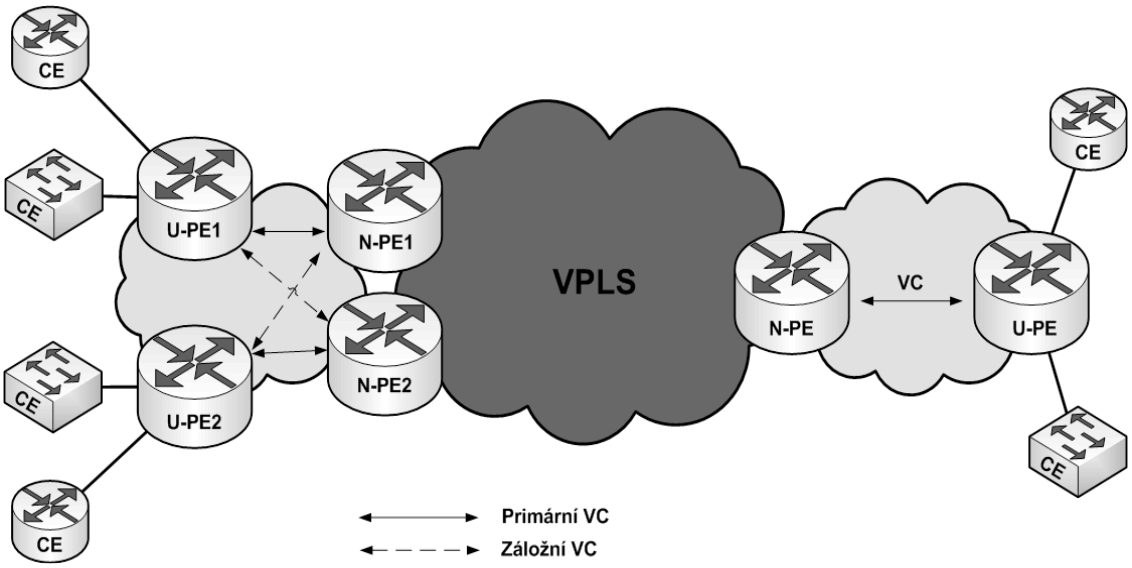



Obr. 7.7 Přístupová vrstva využívající Dot1q tunel

Na obr. 7.7 je zobrazeno toto redundantní řešení pro dvě zákaznické sítě. Směrovač CE1 má zapojen linku pro přenos VLAN A do směrovače poskytovatele U-PE1. Tento směrovač má zajištěnou redundanci do směrovače N-PE1 což je primární cesta a do směrovače N-PE2 což je záložní cesta.

### 7.5.2 H-VPLS s přístupovou vrstvou MPLS

Přístupová vrstva vytvořená službou MPLS potřebuje mít vytvořené virtuální okruhy typu bod-bod mezi směrovači poskytovatele N-PE a směrovači v přístupové vrstvě U-PE. Funkce split horizon musí být zapnuta na rozhranních N-PE směrovače, kde virtuální okruhy vedou k dalším N-PE směrovačům. A vypnuta musí být na rozhranních, kde virtuální okruhy vedou ke směrovačům U-PE. Na obr. 7.8 je zobrazena hierarchická VPLS s přístupovou vrstvou MPLS.




Obr. 7.8 Přístupová vrstva využívající MPLS

Redundance je v tomto případě zaručena vytvořením záložních virtuálních okruhů k redundantním N-PE směrovačům. V tomto případě má směrovač U-PE1na obr. 7.8 primární virtuální okruh se směrovačem N-PE1 a záložní se směrovačem N-PE2. Primární okruhy jsou funkční, dokud nenastane výpadek, jakmile se tak stane, záložní virtuální okruhy se stanou aktivními stejně jako redundantní N-PE směrovač.

# 8. Srovnání technologií AToM a VPLS

Nejdříve zhodnotíme věci, které mají obě technologie stejné, v čem jsou si podobné a následně popíšeme poznatky, ve kterých se obě technologie liší.

Obě tyto technologie zaručují virtuální privátní službu. Obě technologie využívají stejnou strukturu MPLS sítě pro přenos provozu mezi zákaznickými sítěmi. To znamená, že provoz od zákazníka je posílán k hraničnímu směrovači poskytovatele, zde jsou k IP paketům přidány MPLS záhlaví. Nezávisle na technologii se nejdříve přidává značka virtuálního okruhu, ta definuje výstupní hraniční směrovač. Podle této značky, pak může hraniční směrovač usoudit, kterému připojenému okruhu provoz patří. Poté je k IP paketu přidáno další MPLS záhlaví, které definuje jak má paket postupovat v MPLS jádru k cílovému hraničnímu směrovači. Na posledním respektive na předposledním směrovači poskytovatele je značka definující cestu v MPLS jádru odstraněna funkcí Penultimate Hop Popping (PHP), není potřeba značku přenášet do posledního směrovače. IP paketu tedy zbývá jedna značka definující virtuální okruh. Po příchodu k cílovému směrovači se podle této značky určí, do kterého připojeného okruhu zákazníka bude provoz posílán. Mezi hraničními směrovači jsou vytvořeny virtuální okruhy. Oba modely těchto VPN typů se v jádře MPLS chovají zcela podobně.

Technologie AToM vytváří spojení typu bod-bod. To znamená, že tunel vytvořený mezi hraničními směrovači poskytovatele může propojovat pouze dvě sítě zákazníka. Technologie AToM zapouzdřuje do MPLS záhlaví protokoly, které se používají pro spojení LAN-to-LAN, tedy protokoly PPP a HDLC. Dále zapouzdřuje WAN technologie Frame Relay a ATM. Posledním protokolem, který AToM podporuje je Ethernet. Pro přenos protokolů PPP, HDLC, Frame Relay nebo ATM je funkce AToM dostačující. V případě Ethernetu je tato technologie málo využitelná, jelikož nepodporuje více funkcí spojené s LAN segmenty. V tomto případě nastupuje technologie VPLS, která pracuje pouze s Ethernetovými segmenty ve spojení typu bod-více bodů. Přebírá tedy funkci přepínače druhé vrstvy. Podporuje všesměrové a skupinové vysílání, dynamicky se dokáže učit MAC adresy.

Spojení tunelů mezi hraničními směrovači je u technologie AToM přiřazeno fyzickým rozhranním nebo pod-rozhranním. U technologie VPLS se tunely vytvářejí na rozhranní VLAN pro vytvoření všesměrové domény. Jelikož model VPLS se tváří jako přepínač, přebírá i některé jeho funkce, které jsou nezbytnou součástí LAN segmentu. Podporuje protokoly pro snadnější správu LAN sítě, tedy protokoly STP, VTP a CDP. Obě tyto technologie využívají QoS, což je služba bez které by se kvalitní konvergovaná WAN síť neobešla. Obě technologie používají rozdílné způsoby konfigurací virtuálních okruhů. AToM vytváří virtuální okruhy mezi dvěma

směrovači poskytovatele, zatímco VPLS vytváří virtuální okruhy ve full-mash topologii. Tedy musí být vytvořeny virtuální okruhy mezi všemi směrovači, které jsou použity v jedné VPLS instanci. Rozdíl je taky v zařízeních podporující tyto služby. Firma Cisco nabízí podporu technologie AToM už ve svých nižších řadách, nejnižší podporovaná třída je Cisco Series 1861. Na druhou stranu technologie VPLS je podporovaná až od řady Cisco Series 7600.

# 9. Závěr

V této diplomové práci jsou popsány dvě technologie vytvářející virtuální privátní sítě. Nejprve je pospána technologie AToM, její chování, způsob zapouzdření IP paketů v MPLS síti. Dále je popsána konfigurace pro vytvoření jádra, přepínající IP provoz podle značek. Jsou zde uvedeny topologie sítí pro přenos protokolů PPP, HDLC, Ethernet a Frame Relay. U zapojení EoMPLS je možno využít módu Ethernet nebo VLAN. Pro tuto práci jsem zvolil VLAN mód, jelikož u tohoto módu je možné směrovat provoz zákázníka do odlišných destinací. Na druhé straně Ethernet mód vytváří trunk mezi dvěma hraničními směrovači a zapouzdřuje více virtuálních okruhů do jedného tunelu. Dále je zkoumáno zapouzdření Ethernetových rámců pomocí paketového analyzátoru Wireshark. Provoz byl zachycen na třech místech topologie a z nich můžeme vidět techniku zapouzdření, jež využívá MPLS. Zapojení FRoMPLS je v módu DLCI-to-DLCI. Tedy mód kdy dochází k přepínání DLCI na obou koncích tunelu. Paketovým analyzátorem jsou pakety zkoumány také na třech místech topologie.

V další části se věnuji technologii VPLS, tato část je pouze teoretická, uvedené realizace nejsou odzkoušeny v laboratorním prostředí, jelikož vybavení nebylo pro tuto technologii dostačující.

Technologie MPLS je mladá služba, která má mnoho výhod oproti starším WAN technologiím. Má mnoho vlastností, jež můžou ovlivňovat její chování. Poskytovatelé nasazující tuto technologii MPLS, můžou zaručit rychlou konvergovanou síť, jež může přenášet jakýkoliv provoz. Samotná MPLS služba přenáší pouze IP provoz mezi zákaznickými sítěmi.

Technologii AToM můžeme využít pokud zákázníci potřebují přenášet provoz mezi LAN prostřednictvím protokolů PPP a HDLC. Dále je možno přenášet touto službou starší WAN protokoly jako Frame Relay nebo ATM. Pro Ethernet je lepší řešení VPLS, která umožňuje spojení více lokalit a byla vyvinuta přímo pro přenos Ethernetových segmentů.

# Literatura


[1] SIMPSON, W. *Faqs.org* [online]. July 1994. RFC 1661 - The Point-to-Point Protocol (PPP). Dostupné z WWW: http://www.faqs.org/rfcs/rfc1661.html

[2] MARTINI, L.; ROSEN, E. *Faqs.org* [online]. September 2006. RFC 4618 - Encapsulation Methods for Transport of PPP/High-Level. Dostupné z WWW: http://www.faqs.org/rfcs/rfc4618.html

[3] DE GHEIN, Luc. *MPLS Fundamentals*. Indianapolis, IN 46240 USA : Cisco Press, 2007. 607 s. ISBN 1-58705-197-4.

[4] LASSERRE, M.; KOMPELLA, V. *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling* [online]. January 2007. Dostupné z WWW: http://www.faqs.org/rfcs/rfc4762.html

[5] VPLS Deployment Models. In *Layer 2 VPN architectures* [online]. Dostupné z WWW: http://fengnet.com/book/layer%202%20vpn%20architectures/ch15lev1sec2.html

# Seznam příloh

Všechny přílohy jsou uvedeny na CD. Přílohy obsahují výpisy konfigurací jednotlivých zařízení u jednotlivých zapojení.

Příloha A: Výpisy konfigurací ze směrovačů v zapojení PPP over MPLS

Příloha B: Výpisy konfigurací ze směrovačů v zapojení HDLC over MPLS

Příloha C: Výpisy konfigurací ze směrovačů v zapojení Ethernet over MPLS

Příloha D: Výpisy konfigurací ze směrovačů v zapojení Frame Relay over MPLS